UNIVERSIDADE CATÓLICA DE GOIÁS
DEPARTAMENTO DE COMPUTAÇÃO
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

A TECNOLOGIA WI-FI

DANIELA MANRIQUE DE OLIVEIRA

GOIÂNIA, NOVEMBRO 2007

DANIELA MANRIQUE DE OLIVEIRA

TECNOLOGIA WI-FI

TRABALHO DE CONCLUSÃO DE CURSO II apresentado à BANCA EXAMINADORA DA UNIVERSIDADE CATÓLICA DE GOIÁS, para a conclusão do CURSO DE CIÊNCIA DA COMPUTAÇÃO.

Orientador: Prof. Eng. Msc. Wilmar Oliveira de Queiroz

Prof. Eng. Msc Raulino Alves de Castro Neto

Prof. Eng. MBA Piero Martelli

Goiânia, Novembro/2007

DANIELA MANRIQUE DE OLIVEIRA

A TECNOLOGIA WI-FI

TCC II defendido e aprovado em 22 de novembro de 2007, pela Banca Examinador constituída pelos professores da Universidade Católica de Goiás.

Prof. Eng. Msc. Wilmar Oliveira de Queiroz

Prof. Eng. Msc Raulino Alves de Castro Neto

Prof. Eng. MBA Piero Martelli

AGRADECIMENTOS

Primeiramente a Deus que me permitiu chegar até este ponto.

Aos meus pais, que tanto me auxiliaram e me incentivaram na conclusão deste projeto.

Ao meu Professor Orientador Msc. Wilmar Oliveira de Queiroz que, mesmo apesar de todas as minhas dificuldades para redigir este projeto, nunca me desanimou e pelo contrário, sempre me motivou.

Aos amigos que sempre ajudaram ao longo do meu percurso acadêmico e do meu convívio no trabalho, que terminam por ser outra família.

E por fim, a todos os funcionários desta entidade universitária, aos alunos do Curso de Ciência da Computação, aqueles com os quais passei a maior parte de meus dias, superando as dificuldades e aprendendo com as diferenças.

“Não tenho nenhum dom especial.
Sou só apaixonadamente curioso.”

– ALBERT EINSTEIN

RESUMO

É notório o crescimento da comunicação de dados através de redes sem fio. Essas redes permitem uma série de novas funcionalidades para troca de informações, tais como a facilidade de mobilidade entre dispositivos e flexibilidade de conexões, bem como prometem o aumento da produtividade com custos relativamente baixos.

Este trabalho visa estudar o funcionamento de redes sem fio, Redes de Computadores, Topologia de Redes, Camadas, Classificação das Redes, Segurança, outros tipos de tecnologias Wireless – Wi-Fi, protocolos, conceitos e funcionamentos de Wi-Fi e as Configurações de redes sem fio para Windows.

ABSTRACT

It is well-known the growth of the communication of data through nets without thread. These nets allow a series of new functionalities for change of information, such as the mobility easiness between devices and flexibility of connections, as well as they promise the increase of the productivity relatively with costs low.

This work aims to study the operation of wireless networks, networks of computers, Network Topology, Layers, Classification of networks, security, and other types of Wireless technologies, protocols, concepts and workings of Wi-Fi and settings for wireless networks Windows.

LISTAS DE ABREVIATURAS E SIGLAS

AP -	Access Point
BSA -	Basic Set Area
BSS -	Basic Service Set
CCA -	Clear Channel Assessment signal
CCK -	Chip Complementary Code Keying
CSMA/CA -	Carrier Sense Multiple Access with Collision Avoidance
CTS -	Clear-To-Send
DBPSK -	Differential Binary Phase Shift Keying
DCF -	Distributed Coordination Function
DHCP -	Dynamic Host Configuration Protocol
DIFS -	Distributed Interframe Space
DNS -	Domain Name System
DQPSK -	Differential Quadrature Phase Shift Keying
DS -	Distribution System
DSSS -	Direct Sequence Spread Spectrum
EM -	Estação Móvel
ESS -	Extended Service Set
FHSS -	Frequency Hopping Spread Spectrum
GFSK -	Gaussian Frequency Shift Keying
IEEE -	Institute of Electrical and Electronics Engineers
ISM -	Industrial, Scientific, and Medical
LAN -	Local Area Network
MAC -	Media Access Control
MAN –	Metropolitan Area Network
OFDM -	Orthogonal Frequency Division Modulation
PA -	Ponto de Acesso
PAN -	Personal Area Network

PDAs -	Personal Digital Assistant
PPM -	Pulse Position Modulation
QoS –	Quality of Service
SSID -	Service Set Identification
STA -	Wireless LAN Stations
TCP -	Transmission Control Protocol
IP -	Internet Protocol
TKIP -	Temporal Key Integrity Protocol
USB -	Universal Serial Bus
VPN -	Virtual Private Network
WAN -	Wide Area Network
WECA -	Wireless Ethernet Compatibility Alliance
WEP -	Wired Equivalent Privacy
WLAN -	Wireless Local Area Network
WMAN -	Wireless Metropolitan Area Network
WPA -	Wi-Fi Protected Access
WPAN -	Wireless Personal Area Network
WWAN -	Wireless Wide Area Network

A TECNOLOGIA WI-FI

SUMÁRIO

1. Introdução 1
2. Redes de Computadores 3
2.1. Estrutura de uma rede 4
2.2. Topologia de Redes de Computadores 4
2.3 Camadas 7
2.4. Tipos de Rede 7
3. Redes sem Fio 8
3.1 Redes Infra-Estruturadas 8
3.2 Redes Ad Hoc 9
3.3 Vantagens e Desvantagens das Redes sem Fio 9
3.4. Classificação das Redes 10
3.4.1 WPAN 11
3.4.2 WLAN 11
3.4.3 WMAN 11
3.4.4 WWAN 11
3.5. Características dos Meios de Comunicação 12
3.5.1 A tecnologia Wireless 12
3.6. Segurança Wireless 15
3.6.1 A segurança da Rede 16
3.6.2 Os Sistemas Operacionais de Rede 17
3.6.3 Os limites de segurança do protocolo WEP 18
3.7. Outras Tecnologias Wireless 20
3.7.1 Infravermelho 20
3.7.2. Bluetooth 21

3.7.3 Wi-Max 22
3.8. A Arquitetura do 802.11 23
3.8.1 A Camada Física do 802.11 24
3.8.2 O Padrão IEEE 802.11 26
3.8.3 Controles de Rede Wireless 27
3.8.2. Adaptadores de rede 28
4. Wi-Fi 30
4.1. O funcionamento do Wi-Fi 34
4.1.1 Sinais de rádio 35
4.1.1.1 Frequency-Hopping Spread Spectrum (FHSS) 36
4.1.1.2 Direct-Sequence Spread Spectrum (DSSS) 36
4.2 Verificação de erros 38
4.3 Controles de rede wireless 802.11b 38
4.3.1 A camada física 38
4.3.2 A camada MAC 39
4.3.3 Wireless 41
4.4 Adaptadores de rede 41
4.4.1 PC Cards 41
4.4.2 Adaptadores USB 42
4.4.3 Placas de expansão internas 42
4.4.4 Adaptadores internos 43
4.4.5 Compatibilidade de sistema operacional 43
4.4.6 Facilidade de utilização 43
4.5 Segurança 44
4.6 Documentação e suporte técnico 45
4.7 Adaptadores para redes Ad-Hoc 46
4.8 Adaptadores de dupla finalidade 47
4.9 Pontos de acesso 48
4.9.1 LANs wireless puras 48
4.9.2 Múltiplos pontos de acesso 49
4.10 Antenas externas 50

4.10.1 Características da antena 51
4.10.2 Padrão de cobertura 51
4.10.3 Ganho 51
4.10.4 Fator de formação 52
4.11 Instalação e configuração dos pontos de acesso 52
4.11.1 Quantos pontos de acesso? 53
4.11.2 Problemas de interferência 54
4.11.3 Instalando pontos de acesso 55
4.11.4 Comandos de configuração e definições 55
4.11.4.1 Endereço IP 56
4.11.4.2 Máscara de sub-rede 56
4.11.4.3 Canal 56
4.11.4.4 Segurança 57
4.11.4.5 DHCP 57
4.11.5 Múltiplos pontos de acesso 57
6. Conclusão 59
7. Referencias Bibliográfica 60
8. ANEXO I.....62

INTRODUÇÃO

Desde a descoberta das ondas de rádio buscou–se utilizar suas propriedades para a transmissão de dados sem fio, permitindo mobilidade e conexões entre localidades remotas. Do primitivo telégrafo até hoje, busca–se cada vez mais o aumento da taxa de transmissão, otimização da faixa espectral ocupada, baixa taxa de erros, alta disponibilidade da solução, entre outras características que norteiam o "*mundo sem fio*" [1].

As Tecnologias de Redes Sem Fio vêm se tornando uma alternativa viável às redes convencionais permitindo aos seus usuários executar as mesmas tarefas e mais, proporcionando flexibilidade e mobilidade, não apenas dentro das corporações, mas também fora delas.

Para utilizar com mais eficiência a tecnologia wireless, é importante entender o que acontece dentro das caixas que compõem a rede. Este projeto também descreve padrões e especificações que controlam as redes wireless, explicando também como os dados são transportados através da rede de um computador para outro.

A intenção desse trabalho é mostrar o estudo das redes de computadores, suas topologias, camadas, redes sem fio, segurança e principalmente sobre Wi-Fi. Será feita uma abordagem sobre os aspectos legais, vantagens e desvantagens.

Contém uma explicação sobre os conceitos gerais envolvidos com o funcionamento do Windows em uma WLAN e os procedimentos específicos para configurar as ferramentas e recursos de rede em diferentes versões do Windows.

Este trabalho apresenta a seguinte estrutura: no capítulo 2 são apresentados conceitos de Redes de Computadores, Topologia de Redes, Camadas. No capitulo 3 são apresentados Redes sem fio e Classsificação das Redes, segurança, outros tipos de tecnologias Wireless, protocolos. No capítulo 4 conceitos e funcionamentos de Wi-Fi, Capitulo 5 “Configurando redes sem fio para Windows, e a conclusão capítulo 6.

CAPITULO II

REDES DE COMPUTADORES

Cada um dos três últimos séculos foi dominado por uma tecnologia principal. O século XVIII foi a época dos grandes sistemas mecânicos que acompanhavam a Revolução Industrial. O século XIX foi a idade da máquina a vapor. Ao longo do século XX, a tecnologia-chave tem sido a coleta, o processamento e a distribuição da informação.

Entre outros desenvolvimentos, assistiu-se a instalação de redes telefônicas mundiais, a invenção do rádio e da televisão, ao nascimento de computadores e ao lançamento de satélites de comunicação. [1]

As áreas estão convergindo rapidamente, e as diferenças entre coletar, transportar, armazenar e processar informações estão rapidamente desaparecendo. À medida que aumenta a habilidade de coletar, processar e distribuir informações aumenta mais rapidamente a demanda por aplicações ainda mais sofisticadas.

Embora a indústria de computadores seja jovem quando comparada com indústrias como a automotiva e a de transportes aéreos, os computadores têm realizado progresso em um curto espaço de tempo. Durante as suas duas primeiras décadas de existência, os sistemas de computadores eram altamente centralizados, em geral, em uma única e ampla sala.

O velho modelo de um único computador servindo a todas as necessidades computacionais da organização está rapidamente sendo substituído por outro no qual um grande número de computadores separados, mas interconectados, executam essa tarefa. Essas são as chamadas redes de computadores. [1]

Uma série de Padrões Internacionais para a descrição de arquiteturas de redes de computadores foi aceita por toda a indústria de computadores, sendo esses padrões

conhecidos como o Modelo de Referência OSI. Com isso, tem-se que capacitando os computadores de um fabricante a se comunicarem com computadores de outros fornecedores, sem quaisquer problemas de compatibilidade, estimulando ainda mais o uso de redes de computadores.

2.1 ESTRUTURA DE UMA REDE

Uma rede de computadores é formada por um conjunto de computadores autônomos interconectados. Por interconectados, entende-se que eles são capazes de trocar informações entre si, sendo que essa conexão pode ser feita por meio de fios de cobre, por lasers, microondas, etc. É importante ressaltar que uma rede não precisa ser constituída unicamente por computadores, sendo comum à presença de impressoras, scanners e outros dispositivos de rede. [1]

2.2 TOPOLOGIA DE REDES DE COMPUTADORES

As topologias de redes de computadores são compostas abaixo:

Ponto a ponto - É um tipo de configuração física de enlaces (links) de comunicação de dados, onde existem apenas dois pontos de dispositivos de comunicação em cada uma das extremidades dos enlaces, um exemplo esta localizado na figura 1 abaixo. [8]

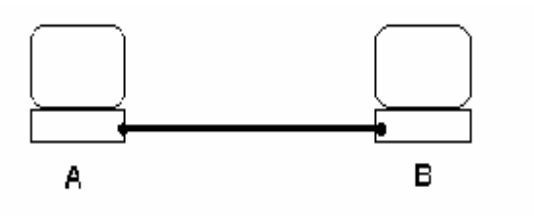

Figura 1: Ponto a ponto

Multiponto - Presença de mais de dois pontos de comunicação utilizando o mesmo enlace que esta sendo representado na figura 2. [8]

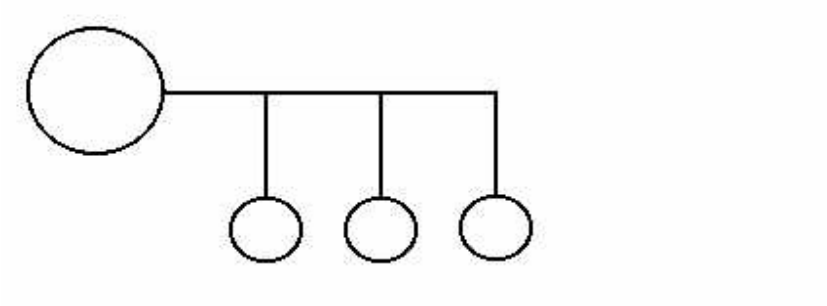

Figura 2: Multiponto

Estrela - Uma rede tem topologia estrela quando um computador se conecta a outro apenas através de um equipamento central concentrador, sem nenhuma ligação direta, nem através de outro computador, um exemplo pode ser encontrado na figura 3. [8]

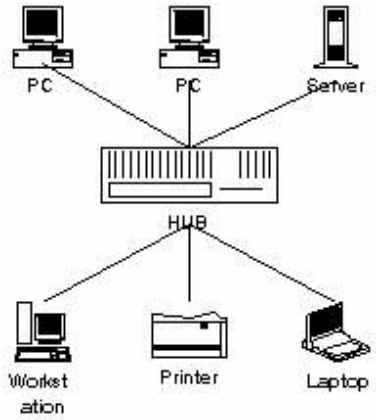

Figura 3: Estrela

Rede em anel - Consiste em estações conectadas através de um circuito fechado, em série, formando um circuito fechado. O anel não interliga as estações diretamente, mas consiste de uma série de repetidores ligados por um meio físico, sendo cada estação ligada à esses repetidores, um exemplo desse tipo de topologia pode ser encontrado na figura 4. O fluxo de informação é unidirecional, existindo um dispositivo HUB que intercepta e gera o fluxo de dados que entra e sai do anel. [8]

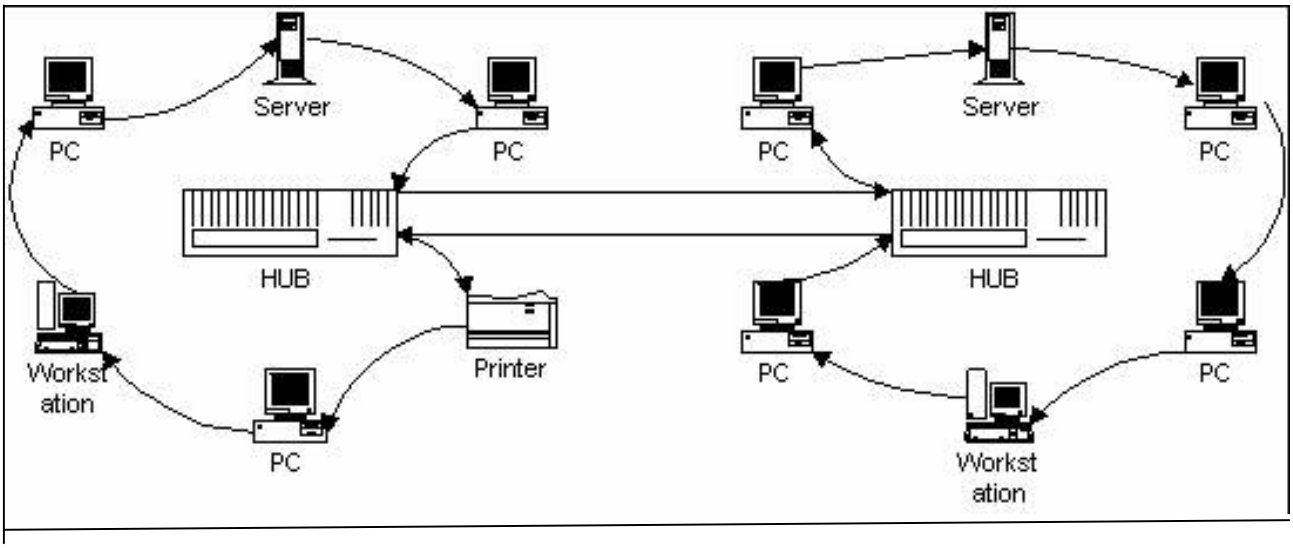

Figura 4: Rede em Anel [8]

Rede em barramento - Como nos computadores, numa rede o barramento é um caminho de transmissão de sinais, estes são lidos pelos dispositivos cujo endereço foi especificado. No caso de uma rede com esta topologia em vez de sinais temos pacotes de dados, cujo cabeçalho contém o endereço do destinatário. Na figura 5 pode ser visualizada uma topologia em barramento, que consiste num cabo com dois pontos terminais e com diversos dispositivos ligados ao barramento (cabo). [9]

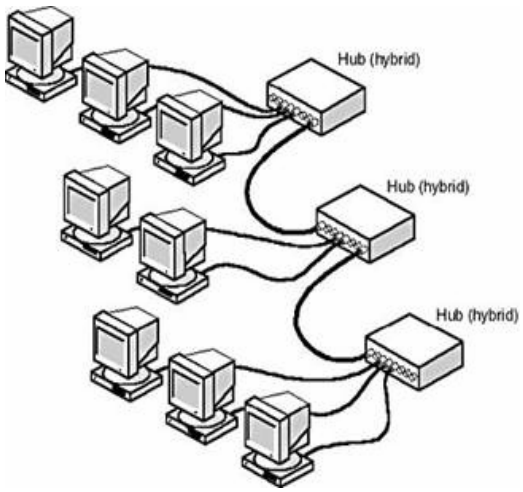

Figura 5: Topologia Estrela-Barramento [9]

2.3. CAMADAS

Para reduzir as complexidades de seu projeto, as redes de computadores são organizadas em camadas ou níveis, que representam diferentes níveis de abstração com funções definidas. Assim cada camada é construída sobre aquela que a antecede. O número de camadas, o nome, o conteúdo e a função de cada camada diferem de uma rede para outra. Entretanto, em qualquer rede, o objetivo de cada camada é oferecer determinados serviços às camadas superiores, protegendo essas camadas dos detalhes de como os serviços oferecidos são de fato implementados, além de também receberem serviços das camadas inferiores. [1]

2.4 TIPOS DE REDES

As redes são classificadas em[1]:

- Redes Locais: São redes em que os computadores localizam-se em uma faixa que varia de poucos metros até alguns quilômetros. É conhecida como *LAN - Local Area Network.*

- Redes Metropolitanas: São redes de computadores onde a distância entre as máquinas começa a atingir distâncias metropolitanas, sendo conhecida como *MAN - Metropolitan Área Network.*

- Redes Geograficamente Distribuídas: Também conhecida como *WAN - Wide Área Network*, esse tipo de rede apareceu devido à necessidade de compartilhamento de recursos entre usuários geograficamente dispersos, sendo que seu custo de comunicação é elevado, uma vez que ela trabalha com enlaces de microondas, satélites, etc.

CAPITULO III

REDES SEM FIO

Alguns conceitos iniciais se fazem necessários para a melhor compreensão do restante do conteúdo aqui apresentado.

3.1 REDES INFRA-ESTRUTURADAS

Tem como característica possuir dois tipos de elementos: As Estações Móveis (EM) e os Pontos de Acesso (PA). Os pontos de acesso são responsáveis pela conexão das estações móveis com a rede fixa, cada ponto de acesso tem o controle de uma determinada área de cobertura (*BSA - Basic Set Area*). O PA realiza tarefas importantes de coordenação das estações móveis em sua área, tais como:

- Aceita ou não uma nova estação na rede;
- Colhe estatística, para realizar gerenciamento do canal e desta forma decidir quando uma estação pode ou não ser controlada por outro ponto de acesso. Sua representação está na figura 6.[11]

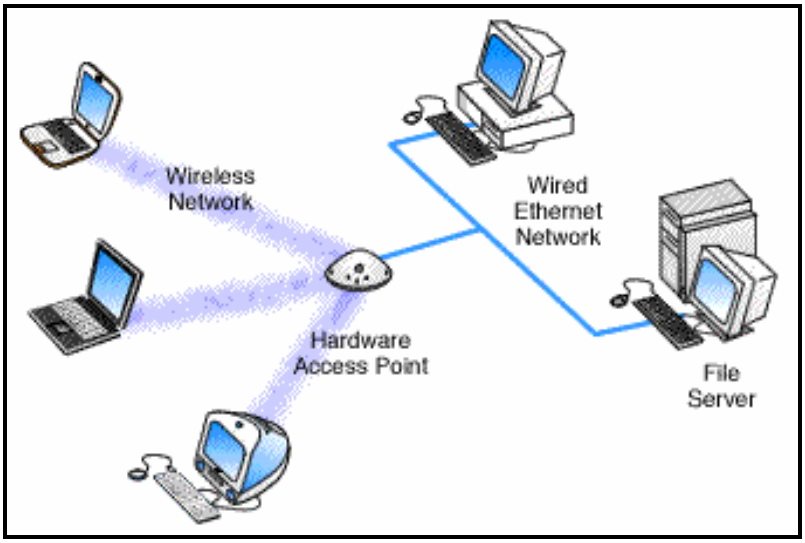

Figura 6: Redes Infra-Estruturada [11]

3.2 REDES AD HOC

As redes Ad Hoc têm como característica não possuir nenhuma infra – estrutura para apoiar a comunicação. Os diversos equipamentos móveis ficam localizados numa pequena área onde estabelecem comunicação ponto a ponto por certo período de tempo. A figura 7 representa a rede Ad Hoc. [11]

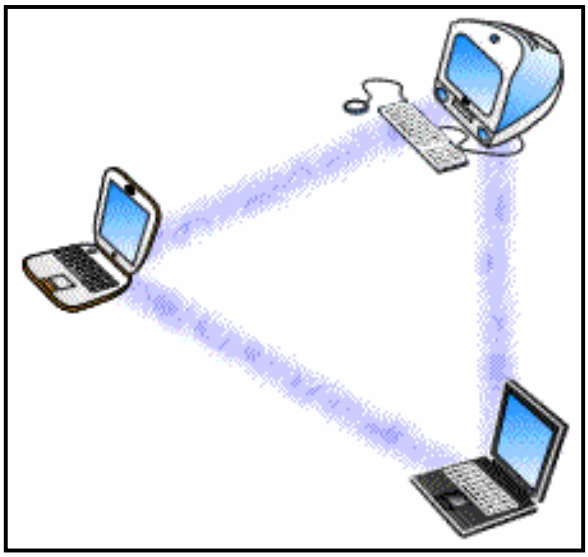

Figura 7: Redes Ad Hoc [11]

3.3 VANTAGENS E DESVANTAGENS DAS REDES SEM FIO

As redes apresentam algumas vantagens: [1]

- Flexibilidade: dentro da área de cobertura, uma determinada estação pode se comunicar sem nenhuma restrição. Além disso, permite que a rede alcance lugares onde os fios não poderiam chegar;
- Facilidade: a instalação pode ser rápida, evitando a passagem de cabos através de paredes, caneletas e forros, portanto uso mais eficiente do espaço físico;

- Redução do custo agregado: mesmo mais dispendiosa que uma rede cabeada, as redes sem fio agregam vantagens como: melhor utilização de investimentos em tecnologias existentes como laptops, rede de dados e voz, aplicativos, agilidade nas respostas aos clientes;
- Topologias diversas: podem ser configuradas em uma variedade de topologias para atender a aplicações específicas. As configurações são facilmente alteradas, facilidade de expansão, manutenção reduzida.

Em contrapartida, apresentam também algumas desvantagens: [1]

- Qualidade de serviço: a qualidade do serviço provido ainda é menor que a das redes cabeadas. Tendo como principais razões para isso a pequena banda passante ocasionada pelas limitações da transmissão e a alta taxa de erro decorrente das interferências;
- Custo: o preço dos equipamentos de Redes sem Fio é mais alto que os equivalentes em redes cabeadas;
- Segurança: intrinsecamente, os canais sem fio são mais suscetíveis a interceptores não desejados. O uso de ondas de rádio na transmissão de dados também pode interferir em outros equipamentos de alta tecnologia, como por exemplo, equipamentos utilizados em hospitais.
- Baixa transferência de dados: embora a taxa de transmissão das Redes sem Fio esteja crescendo rapidamente, ela ainda é muito baixa se comparada com as redes cabeadas.

3.4 CLASSIFICAÇÃO DAS REDES

As redes são classificadas em[3]:

3.4.1 WPAN

Wireless Personal Area Network ou rede pessoal sem fio. Normalmente utilizada para interligar dispositivos eletrônicos fisicamente próximos. Este tipo de rede é ideal para eliminar os cabos usualmente utilizados para interligar teclados, impressoras, telefones móveis, agendas eletrônicas, computadores de mão, câmeras fotográficas digitais, mousars e outros. Nos equipamentos mais recentes é utilizado o padrão Bluetooth para estabelecer esta comunicação, mas também é empregado raio infravermelho (semelhante ao utilizado nos controles remotos de televisores).

3.4.2 WLAN

Wireless Local Area Network ou rede local sem fio. Abrangência de uma rede não ultrapassa algumas dezenas ou centenas de metros, situando-se, normalmente, dentro de um edifício.

3.4.3 WMAN

Wireless Metropolitan Area Network. Redes que abarcam a área de uma grande cidade ou região urbana, interligando determinadas entidades ou instituições que necessitam de manter entre si um sistema de comunicações de dados (como, por exemplo, as entidades administrativas ou policiais de uma grande cidade).

3.4.4 WWAN

Wireless Wide Area Network Redes de computadores ou conjunto de redes cuja abrangência se entende por toda uma região, várias regiões, vários países ou até no Mundo (como é o caso da Internet).

3.5 CARACTERÍSTICAS DOS MEIOS DE COMUNICAÇÃO

O termo "meio de comunicação" refere-se ao instrumento ou à forma de conteúdo utilizados para a realização do processo comunicacional.

3.5.1 A TECNOLOGIA WIRELESS

A palavra *wireless* provém do inglês: wire (fio, cabo); less (sem); ou seja: sem fios. Wireless caracteriza qualquer tipo de conexão para transmissão de informação sem a utilização de fios ou cabos. Uma rede *wireless* é um conjunto de sistemas conectados por tecnologia de rádio através do ar. Dentro deste modelo de comunicação, pode-se enquadrar várias tecnologias, como Wi-Fi, InfraRed (infravermelho), Bluetooth e Wi-Max. [3]

Aplica-se esse conceito também em muitos outros aparelhos, como por exemplo, o controle remoto da TV, aparelhos de som, telefones celulares. Pode ser dividida de duas formas: Indoor, quando se trata, por exemplo, da comunicação em rede de computadores que estão numa mesma sala ou prédio, ou Outdoor, quando há necessidade de uma comunicação estendida, ou seja, numa grande empresa ou mesmo num campus universitário, onde há necessidade de comunicação com outros prédios situados num mesmo local geográfico.

Para que se possa entender melhor sobre a arquitetura/topologia, é necessário entender alguns conceitos básicos: [4].

- **BSS** (*Basic Service Set*) - Corresponde a uma célula de comunicação da rede sem fio, ou a região de retransmissão.

• **STA** (*Wireless LAN Stations*) - São as estações de trabalho que se comunicam entre si dentro da BSS.

• **AP** (*Access Point*) - Nó que coordena a comunicação entre as STAs dentro da BSS. Funciona como uma ponte de comunicação entre a rede sem fio e a rede convencional. Ex: Antena de comunicação.

• **DS** (*Distribution System*) - Corresponde ao backbone da WLAN, realizando a comunicação entre os APs.

• **ESS** (*Extended Service Set*) - Conjunto de células BSS cujos APs estão conectados a uma mesma rede convencional. Nestas condições uma STA pode se movimentar de uma célula BSS para outra permanecendo conectada à rede. Este processo é denominado de Roaming.

• **IBSS** (Independent *Basic Services Set*) - Um BSS que não está ligado a uma base é visto como um BSS independente (IBSS) ou como uma rede Ad-Hoc, que é uma rede onde as estações comunicam-se apenas utilizando peer-to-peer. Não existe uma base e não é dada, por ninguém, a permissão para falar, a maioria destas redes é espontânea e podem ser criadas rapidamente. As redes IBSS têm como características o fato de serem limitadas tanto em tempo como em espaço. Uma vez ligado um BSS a uma rede, esta se une à infra-estrutura da rede.

A Figura 8 apresenta, de forma esquemática, os componentes de uma ESS e de uma IBSS.

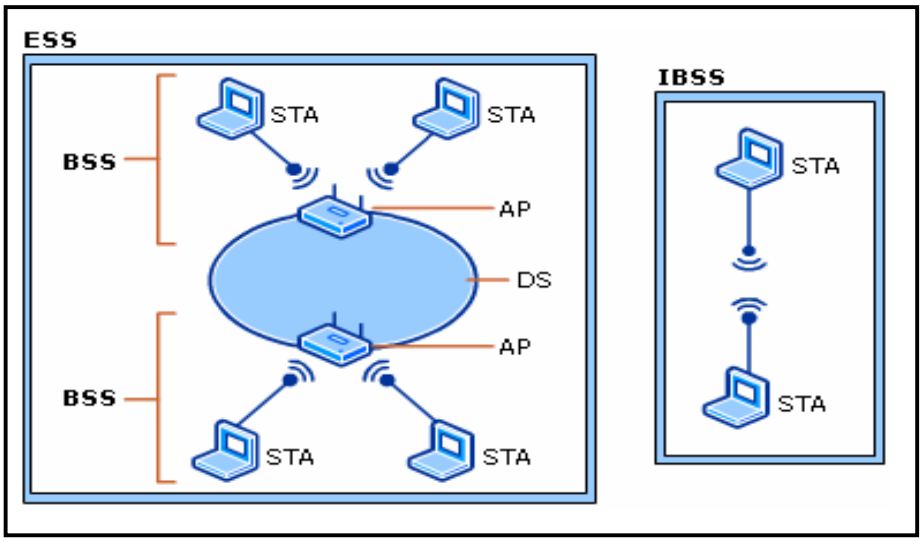

Figura 8: Componentes ESS e IBSS [9]

Segue um modelo simples de funcionamento de uma rede *Wireless* na figura 9:

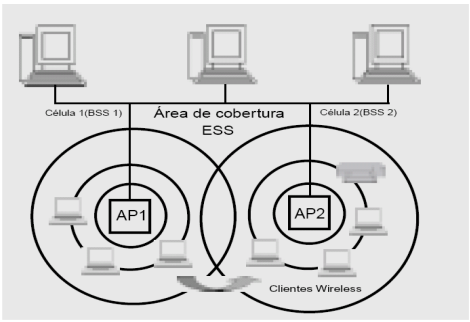

Figura 9: Esquema Simples de uma *Wireless* Lan [9]

No 802.11 existem dois tipos de redes sem fio: *ad-hoc* ou infra-estruturada. Uma rede *adhoc* é composta somente por estações dentro de um mesmo BSS que se comunica entre si sem a ajuda de uma infra-estrutura. Qualquer estação pode estabelecer uma comunicação direta com outra estação no BSS sem a necessidade que a informação passe por um ponto de acesso centralizado. O padrão 802.11 refere-se a uma rede *ad-hoc* como um BSS

independente. Já em uma rede infra-estruturada, é utilizado um ponto de acesso que é responsável por quase toda a funcionalidade de rede. De modo a aumentar a cobertura de uma rede infra-estruturada, vários pontos de acesso podem ser interligados através de um *backbone* chamado sistema de distribuição (*distribution system*). O conjunto dos pontos de acesso e dos sistemas de distribuição é definido com um conjunto estendido de serviços (ESS - *Extended Service Se). [1]*

3.6 SEGURANÇA EM REDES *WIRELESS*

A segurança em redes *wireless* é um assunto tratado ainda de forma muito delicada, tanto pelos que utiliza da tecnologia, quanto pelos fabricantes de equipamentos. Segurança, apesar de ser um item fundamental em qualquer projeto de rede, tem sido tratado com certo descaso pelas pessoas que estão montando uma pequena rede. Apesar dos recursos de segurança atual não serem invioláveis, é sempre bom garantir, ao máximo, que seu ambiente e possível dados estejam bem guardados, bem protegidos.

A questão da segurança é o grande desafio das tecnologias *wireless* atuais. Se já era difícil garantir e proteger redes convencionais, imagine conseguir isso com informações voando pelo ar, de um lado para outro. Sendo que não é uma tecnologia totalmente segura, toda e qualquer medida de segurança ainda que simples, sempre é bem vinda.

Qualquer usuário que não apresente um conhecimento muito avançado sobre o assunto, pode adotar medidas básicas para melhorar a segurança de uma rede *wireless*, o que na maioria das vezes acaba não acontecendo, favorecendo e criando um ambiente ideal para os hackers.[5]

O que realmente é necessário saber para que a rede sem fio implementada esteja com o nível correto de segurança? Primeiramente é preciso conhecer os padrões disponíveis, o que eles podem oferecer e então, de acordo com a aplicação, política de segurança e objetivo, implementar o nível correto e desejado. É preciso entender, avaliar bem as alternativas e

então decidir de acordo com a experiência e as características disponíveis nos produtos que vão ser utilizados, objetivando assim o melhor custo.

Como já mencionado anteriormente, a segurança *wireless* é um grande desafio ainda na área de *wireless*. Com tempo e acesso suficientes, um hacker persistente provavelmente conseguirá invadir seu sistema *wireless*. Ainda assim, podem ser tomadas algumas atitudes para dificultar ao máximo o acesso de intrusos. [6]

O padrão IEEE 802.11 apresenta o serviço de segurança dos dados através de dois métodos: autenticação e criptografia. Ele define duas formas de autenticação: open system e shared key. Independente da forma escolhida, qualquer autenticação deve ser realizada entre pares de estações, jamais havendo comunicação multicast. As formas de autenticação previstas são: [2]

- **Autenticação Open System**: sistema de autenticação padrão. Qualquer estação será aceita na rede, bastando requisitar uma autorização. É um sistema de autenticação nulo. A autenticação Open System foi desenvolvida com a finalidade de buscar redes que não precisam de segurança para autenticidade de dispositivos. Nenhuma informação sigilosa deve trafegar nessas redes já que não apresenta qualquer proteção.

- **Autenticação Shared key**: onde ambas as estações (requisitante e autenticadora) devem compartilhar uma chave secreta. A forma de obtenção desta chave não é especificada no padrão, ficando a cargo dos fabricantes a criação deste mecanismo. A troca de informações durante o funcionamento normal da rede é feita por meio da utilização do protocolo WEP.

3.6.1 A Segurança da Rede

Os requisitos mínimos de segurança de uma rede implicam em que um determinado recurso (informação, equipamento, etc.) somente pode ser acessado por quem de direito e da

maneira prevista. Dessa forma, uma pessoa não autorizada não pode, sob nenhuma hipótese, alterar ou mesmo ler uma informação à qual ele não tenha direito. Além disso, é necessário garantir a integridade dos recursos da rede, de modo a impedir danos e minimizar eventuais desastres que possam acontecer. Para tal, é necessária a adoção de regras estritas de segurança e rotinas rígidas de backup.

Duas ameaças atuais preocupam mais do que tudo os administradores sérios de redes: pirataria e vírus. Nos dois casos, toda rigidez é necessária, incluindo o uso de estações sem drives (embora com disco rígido) ou vacinas, auditorias periódicas e punições severas a quaisquer quebras de regras de segurança. Outro procedimento essencial é a adoção de chaves (também chamadas de contas) com uso restrito e exigência de senhas. Essas senhas não podem ser divulgadas, devendo ser periodicamente alteradas pelo usuário.

Caso a rede deva fornecer operação ininterrupta, deve ser levada em consideração a tolerância à falhas do SORs. Os melhores SORs oferecem no mínimo duplicação de discos, chegando, nos melhores, até à duplicação total de servidores. [6]

3.6.2 Os Sistemas Operacionais de Rede

Existem muitas opções de SORs, apesar do mercado brasileiro ser relativamente restrito. Em compensação, os melhores produtos mundiais estão disponíveis, não havendo assim motivo para maiores preocupações.

Windows para WorkGroups - Rede ponto-a-ponto da Microsoft, oferece um desempenho aceitável e pouca segurança. Domina cerca de 4% do mercado. Personal NetWare - Rede ponto-a-ponto da Novell, vem embutida no Novell DOS 7.0, e possui um desempenho fraco e alguma segurança. Domina cerca de 2% do mercado. Lantastic - A melhor e mais utilizada das redes ponto-a-ponto. Tem um bom desempenho e uma segurança razoável. Domina 6% do mercado. NetWare 3.x - Rede baseada em servidor da Novell, é a mais utilizada no mundo. Oferece excelente desempenho, grande segurança e uma confiabilidade

legendária. Sua administração e configuração são excelentes para redes pequenas e médias, com poucos servidores. Abrange cerca de 52% do mercado mundial. [6]

NetWare 4.x - Rede baseada em servidor da Novell, é uma evolução da 3.x. Oferece como destaque um serviço de diretórios distribuído que garante, em uma rede com vários servidores, que todo e qualquer servidor conhece todos os recursos e chaves e pode validar senhas e direitos de acesso, tornando a rede independente de uma máquina em si. Além disso, possui avançados recursos de acesso a disco como compactação, migração de dados e subalocação de blocos os quais melhoram muito o já ótimo desempenho do acesso a disco. Oferece ainda grande tolerância à falhas, de espelhamento de discos até duplicação total de servidores. Ainda não suporta multiprocessamento. O NetWare 4.x domina cerca de 9% do mercado mundial. [5]

Windows NT - Sistema Operacional multitarefa da Microsoft, é tipicamente um servidor de aplicações, apesar de existirem instalações de rede baseadas em NT. Possui bom desempenho de acesso a disco, incluindo espelhamento de discos (de servidores não), subalocação de blocos e recursos avançados de segurança. Emula servidores NetWare 3.x (não compatível com os serviços de diretório distribuídos do NetWare 4.x) com facilidade, para facilitar eventuais migrações. Não possui serviços de diretório, apenas o conceito de domínios. Suporta também multiprocessamento. O Windows NT, que está tentando assumir uma parte dos mercados NetWare e Unix, domina cerca de 7% do mercado de redes.

Unix - Produzido por vários fabricantes, é amplamente utilizado para aplicações críticas, onde segurança, desempenho e confiabilidade sejam essenciais. É de instalação e administração relativamente complexas se comparado às demais opções.

3.6.3 Os limites de segurança do protocolo WEP

Os principais defeitos do protocolo de segurança Wired Equivalent Privacy são os que seguem - a dimensão do vetor de iniciação é demasiado curta, a união do vetor de iniciação

e da chave de encriptação não é boa e, sobretudo, o mecanismo de encriptação RC4 apresenta chaves fracas.

Os dois primeiros defeitos permitem a desencriptação dos pacotes sem conhecer a chave de encriptação. As chaves fracas do RC4 permitem chegar à chave de encriptação - para isso, basta escutar suficientemente o tráfego. Encontram-se assim várias chaves fracas para atacar. Este defeito é utilizado pelos softwares de cracking (Aisnort e Wepcrack, entre outros) disponíveis na Web. O WEP possui ainda outra falha de peso - o sistema de autenticação por pacotes. Como se baseia numa assinatura do pacote por segmentação linear, é fácil deduzir um pacote forjado partindo de um pacote encriptado e bem formado. [6]

O WPA, que substitui o padrão existente WEP (Wired Equivalent Privacy), adota TKIP - Temporal Key Integrity Protocol, tecnologia que gera novas chaves de segurança para cada 10K de dados transmitidos pela rede, dificultando assim o acesso às informações.

Outro aparelho muito comum no mundo Wi-Fi é o access point (A.P.). É ele quem transforma o tráfego de rede em sinal de rádio, permitindo que outros dispositivos, igualmente equipados com Wi-Fi, possam se conectar a ele. Um dos assuntos mais discutidos e polêmicos em torno do Wi-Fi é a segurança. Como garantir a segurança de informações que trafegam pelo ar, atravessando paredes? Diferente das redes convencionais com cabos, o sinal de rádio de redes Wi-Fi não obedece aos limites físicos do escritório, residência ou empresa, sendo facilmente captado e/ou interceptado e/ou manipulado por estranhos próximos do ambiente de rede, em andares diferentes do prédio ou mesmo, em quarteirões próximos, dependendo da sorte do wardriver.

Para garantir um nível maior de segurança, é necessário se proteger com formas de encriptação, filtros e chaves de segurança, evitando assim que intrusos tenham acesso aos seus dados - mesmo que a pessoa esteja dentro da área de cobertura do sinal. No entanto, chaves do tipo WEP não são muito seguras, pois podem ser facilmente "quebradas" por

pessoas que tenham algum conhecimento sobre o assunto. O ideal é usar encriptação do tipo WPA, que dão uma segurança maior.

Para garantir a segurança da rede sem recorrer exclusivamente ao standard WEP (com lacunas nesta área), é conveniente seguir de perto os trabalhos de normalização do grupo IEEE 802.11i; [2]

Mais prosaicamente, a implementação de uma VPN (Rede Privada Virtual) já garante a segurança de uma infra-estrutura rádio Wi-Fi.

3.7 AS DEMAIS TECNOLOGIAS *WIRELESS*

Além da rede simples conhecida como Wi-Fi, também existem outras soluções de rede sem fio, como Infravermelho, Bluetooth e Wi-MAX. Todas elas serão apresentadas com mais detalhes nesse tópico. [7]

3.7.1 Infravermelho

Meio de comunicação usado em muitos eletrodomésticos e que vem sendo usado há muito tempo. Como exemplo de uso dessa tecnologia pode ser citado: a televisão, som e vídeo cassete que apresentam controles remotos que utilizam do infravermelho para enviar os sinais ao receptor que está presente nesses eletrodomésticos.

Hoje em dia é muito utilizado em dispositivos móveis como PDAs e aparelhos celulares, onde os dois trabalhando juntos permitindo por exemplo, o acesso a Internet, onde eles se comunicam entre si e o celular funciona como um modem que envia os sinais da conexão para os Palmtops permitindo visualizar a Internet nesses dispositivos.

Seu funcionamento ocorre da seguinte forma: o emissor envia um feixe de raios infravermelhos (imperceptíveis a olho nu) que são capturados por um dispositivo sensível

onde à faixa de radiação é então convertida em forma de corrente elétrica. Para que ocorra a troca de informações entre os dois dispositivos, os mesmos devem apresentar um transmissor e um receptor de feixe de raios. Também é necessário que ambas conheçam a linguagem de comunicação empregada, para que isso ocorra os meios devem obedecer a um conjunto de regras denominado protocolo de comunicação. No caso do infravermelho ele utiliza como protocolo de comunicação o IrDA (*Infrared Data Association*).

A velocidade de transmissão nessa tecnologia varia ente 9.600 bits por segundo a 4 Mb/s (megabits por segundo).

Sua desvantagem está no fato de que apresenta baixa capacidade de transmissão de dados, de não ser capaz de atravessar objetos opacos, e a transmissão só pode ocorrer de um único emissor para um único receptor, ou seja, impossibilidade de troca simultânea de dados em vários dispositivos.

3.7.2. Bluetooth

Idealizado em 1998 por um grupo de cinco empresas: Ericson, IBM, Intel, Nokia e Toshiba, com a finalidade de eliminar o uso de cabos para conectar os aparelhos. O objetivo principal dessa tecnologia é criar um meio de comunicação que seja capaz de transpor obstáculos que estão entre o transmissor e o receptor a pequenas distâncias.

Ex: Celulares, fones de ouvido, computadores, teclados, microfones.

A principal vantagem dessa transmissão em relação ao infravermelho é que permite que até oito dispositivos comuniquem entre si. Também não exige um campo de visada direta entre o transmissor e receptor. Apesar de apresentar um alcance de sinal pequeno em torno de 10 metros, o Bluetooth apresenta características que diminuem a interferência que é causada por outras transmissões que trabalham na mesma freqüência, tendo como características,

uma potência de sinal limitada a 1mW, reduzindo o alcance dos sinais, também a alta velocidade de troca de freqüências, são 1.600 vezes por segundo.

O Bluetooth é considerado pelo IEEE 802.15 como uma WPAN (*Wireless Personal Área Network*), ou seja, um meio de extensão de portas para comunicação entre dispositivos específicos.

Essa tecnologia estabelece a comunicação entre dispositivos por meio de uma técnica conhecida como spread-spectrum frequency hopping, a qual permite que dois dispositivos iniciem a troca de informações sem que seja necessária a intervenção do usuário. Essa transmissão é do tipo um para muitos, onde um dispositivo chamado de mestre pode se comunicar simultaneamente com até sete outros dispositivos denominados escravos.

Uma rede Bluetooth recebe o nome de piconet, onde a comunicação ocorre somente entre mestre e escravos. Além da comunicação entre alguns dispositivos de computador, é utilizado também para troca de arquivos e compartilhamento de conexão com a Internet. A figura 10 mostra um exemplo.

Figura 10: notebook conectado em rede por um transmissor bluetooth [7]

3.7.3 Wi-MAX

Conhecido também como WMAN (*Wireless* Metropolitan Área Network), nome comercial para o padrão IEEE 802.16. A principal vantagem em relação ao Wi-Fi refere-se a taxa de

transferência de até 75 Mbps, com um raio de alcance de quase 50 Km em área livre e 8 a 10 Km em área de alta densidade populacional. [2]

A desvantagem com relação ao Wi-Fi, é referente ao seu alto custo para implantação, onde o Wi-Fi é centenas de vezes mais barato do que o WiMax. Muitas empresas de telefonia e que fornecem acesso à internet já tem feito testes para verificar se essa tecnologia pode vir a substituir os cabos par de cobres, para distribuir o sinal de internet.

O Wi-MAX está numa constante evolução, onde os padrões criados para essa tecnologia já tiveram diversas modificações em sua composição de forma a trazerem melhoramentos tanto em nível de custo como melhoria em aspectos operacionais e funcionais. Atualmente a mesma trabalha no padrão 802.16e, que vem trazer uma abrangência maior na área de transmissão, permitindo uma conectividade em velocidade de até 100 Km/h. [7].

3.8 A ARQUITETURA DO 802.11

A seguir mostra-se a arquitetura do 802.11 e adaptadores.

A arquitetura do IEEE 802.11 consiste em vários componentes que interagem para prover uma rede local sem-fio com suporte à mobilidade de estações de modo transparente para as camadas superiores. [2]

O conjunto básico de serviços (BSS - Basic Service Set) é o bloco fundamental de construção da arquitetura do 802.11. Um BSS é definido como um grupo de estações que estão sobre o controle direto de uma única função de coordenação, que determina quando uma estação pode transmitir e receber dados.

3.8.1 A Camada Física do 802.11

O padrão 802.11 define três tipos de camada física: espalhamento de espectro por salto em freqüências (FHSS - Frequency Hopping Spread Spectrum), espalhamento de espectro por seqüência direta (DSSS - Direct Sequence Spread Spectrum) e infravermelho. Todas as camadas físicas do 802.11 incluem a provisão de um sinal de avaliação de canal livre (CCA - Clear Channel Assessment signal) que é utilizado pela subcamada MAC para indicar se o meio está livre. [2]

O FHSS é uma técnica de espalhamento de espectro que divide a banda passante total em vários canais de pequena banda e faz com que o transmissor e o receptor sintonizem em um desses canais por certo tempo e depois saltem para outro canal. Com isso, permitem-se a coexistência de várias redes em uma mesma área através da separação dessas redes por diferentes padrões pseudo-aleatórios de uso do canal chamados seqüências de saltos. O FHHS usa a banda ISM (Industrial, Scientific, and Medical) de 2,4000 a 2,4835 GHz. Nos EUA e em quase toda a Europa, são definidos 79 canais. O primeiro canal tem uma freqüência central de 2,402 GHz e os canais subseqüentes estão separados por 1 MHz. Cada canal possui uma banda de 1 Mbps. Três diferentes conjuntos com 26 seqüências de saltos são definidos. As diferentes seqüências de saltos permitem que vários BSSs coexistam em uma mesma área geográfica e os três conjuntos de saltos existem para evitar períodos de colisões entre diferentes seqüências de saltos em um conjunto.

O acesso básico de 1 Mbps usa uma modulação gaussiana por chaveamento de freqüência (GFSK - Gaussian Frequency Shift Keying) de dois níveis, na qual o dado passa por um filtro gaussiano em banda base e é modulado em freqüência (um 1 lógico é codificado usando uma freqüência $F_c + f$ e um 0 lógico usa uma freqüência i ou j). A taxa de acesso opcional de 2 Mbps usa um GFSK de quatro níveis, no qual dois bits são codificados por vez usando quatro freqüências.

O DSSS – (Direct Sequence Spread Spectrum) é um método alternativo de espalhamento de espectro, no qual códigos são separados. O DSSS também usa a banda ISM de 2,4 GHz.

A taxa básica de 1 Mbps é gerada através de uma modulação diferencial binária por chaveamento de fase (DBPSK - Differential Binary Phase Shift Keying) e a taxa de 2 Mbps usa uma modulação diferencial quaternária por chaveamento de fase (DQPSK - Differential Quadrature Phase Shift Keying). O espalhamento é feito através da divisão da banda disponível em 11 subcanais, cada um com 11 MHz, e do espalhamento de cada símbolo de dados usando uma seqüência de Barker de 11 chips. [2]

BSSs sobrepostos ou adjacentes podem operar ao mesmo tempo sem interferências se a distância entre as freqüências centrais de cada BSS for de pelo menos 30 MHz. Logo, somente dois BSSs sobrepostos ou adjacentes podem ser utilizados sem interferência.

A especificação de infravermelho utiliza comprimentos de onda de 850 a 950 nm. O infravermelho foi projetado para ser usado em áreas fechadas e opera com transmissões não direcionadas com alcance máximo de aproximadamente 10 m caso não existam fontes de calor ou luz do sol interferindo ou 20 m caso sejam utilizados receptores mais sensíveis. As estações podem receber dados em suas linhas de visada e por transmissões refletidas. A codificação da taxa básica de 1 Mbps é realizada através de uma modulação por posição de pulso (PPM - Pulse Position Modulation), na qual quatro bits de dados são mapeados em 16 bits codificados para transmissão. A taxa opcional de 2 Mbps usa uma 4-PPM, na qual dois bits de dados são mapeados em 4 bits codificados para transmissão.

Os padrões 802.11a e 802.11b alteram a camada física do 802.11 para prover taxas de transmissão mais altas. O padrão 802.11b especifica taxas de transmissão mais altas na banda de 2,4 GHz, através da alteração de alguns pontos da norma básica 802.11. Taxas de 1, 2, 5,5 e 11 Mbps são providas nesse padrão através do uso de um chaveamento de código complementar (CCK - chip Complementary Code Keying) no DSSS. O padrão 802.11a utiliza a banda de 5 GHz para poder prover bandas de até 54 Mbps. Esse padrão também altera a norma básica 802.11 em alguns pontos. A camada física utiliza uma multiplexação por divisão ortogonal em freqüência (OFDM). O sistema usa 52 subportadoras que são moduladas usando BPSK ou QPSK, modulação 16-QAM (Quadrature Amplitude Modulation) ou 64-QAM.

3.8.2 O Padrão IEEE 802.11

No protocolo 802.11 o mecanismo fundamental de acesso ao meio é chamado de DCF - Distributed Coordination Function. Este mecanismo é baseado em um esquema de acesso aleatório usando detecção de portadora evitando-se colisões (carrier sense multiple access with congestion avoidance).Neste protocolo sempre que uma estação tem algum pacote para transmitir, ela monitora a atividade do canal, se o canal estiver ocioso por um período maior que o tempo entre quadros distribuído (DIFS - Distributed Interframe Space), a estação transmite o pacote. Senão, ela monitora o canal até que o canal esta ocioso por um período de tempo igual a DIFS e então inicia um contador de duração aleatória (backoff) antes de iniciar sua transmissão tentando minimizar a probabilidade de uma nova colisão, além disso, para que uma única estação não monopolize o canal, esta precisa iniciar seu contador sempre que transmitir dois ou mais pacotes seguidos. [2]

Como uma estação não tem como detectar se houve uma colisão ou não, já que ela é incapaz de transmitir e "escutar" o canal simultaneamente, um ACK é transmitido pela estação de destino logo após um curto período de tempo chamado de SIFS - Short Interframe Space sempre que um pacote é recebido sem erros. Se após o período de tempo igual ACKtimeout um ACK não for recebido, a estação transmissora sabe que houve uma colisão ou uma perda e reagenda a transmissão de acordo com o tamanho da janela de backoff.

Por razões de eficiência, a DCF usa um modelo de tempo segmentado onde uma estação só transmite no inicio de cada segmento e a duração de cada segmento deve ser suficiente para que todas as estações detectem uma transmissão de uma outra estação.

A Função DCF adota um esquema de backoff aleatório. A cada início de transmissão, é inicializado um temporizador com um valor aleatório uniformemente distribuído entre (0, ω –1), onde ω é o tamanho da janela de contenção, e depende do número de tentativas frustradas de transmissão. Na primeira tentativa, ω tem tamanho igual a CWmin que é o

menor tamanho possível de uma janela de contenção. A cada vez que ocorre uma colisão o tamanho da janela de contenção dobra até o valor máximo CWMAX onde CWMAX = 2m CWmin . Este aumento da janela da contenção seria uma forma de fazer com que as estações "entendessem" o comportamento da rede, e se a rede estiver permanente ocupada, volta a tentar mais tarde, se ela estiver muito ociosa transmite logo. Este contador é decrementado sempre que canal está desocupado, quando uma outra transmissão inicia sua transmissão o contador é "congelado" e só é reativado quando o canal fica inativo por um período igual a DIFS.

O padrão 802.11 tem duas formas de operação: o modo descrito acima chamado de modo básico, e o modo de reserva onde cada estação após sentir o canal livre por um tempo igual a DIFS, seguir as regras de backoff descritas anteriormente, ao invés de transmitir seus dados úteis envia um quadro de reserva (reservation request RTS) contendo a duração do pacote de dados endereçado a estação de destino, se a estação de destino recebe este RTS corretamente, ela espera um tempo igual a SIFS e envia um quadro chamado STS - Clear-To-Send indicando que a estação que fez o pedido pode enviar os dados. Após um tempo igual a SIFS a estação que recebeu o CTS inicia a sua transmissão. Uma estação pode operar simultaneamente nos dois modos de operação.

3.8.4 Controles de Rede *Wireless*

O padrão 802.11 especifica o protocolo de controle de acesso ao meio (MAC) e diferentes camadas físicas de alcance e velocidades diversas. Avanços recentes nas técnicas de processamento de sinais permitem que se atinjam taxas de transmissão de até 54 Mbps no padrão 802.11a que opera na banda de 5 GHz. Apesar do aumento contínuo da capacidade dessas redes, as especificações atuais oferecem um suporte limitado à QoS - Qualidade de Serviço.[3]

Mais especificamente, a subcamada MAC do 802.11 oferece, em uma configuração com infra-estrutura, um método centralizado de controle de acesso baseado em consulta, onde os

pontos de acesso são responsáveis pela alocação de banda passante e pela limitação da latência das estações.

O desempenho deste modo de acesso está diretamente ligado aos algoritmos de consulta utilizados, os quais buscam um compromisso entre a eficiência na utilização da banda passante e a capacidade em oferecer garantias estritas de desempenho aos tráfegos sensíveis ao tempo.

Numa configuração de rede sem infra-estrutura, ou ad-hoc, o controle distribuído de acesso ao meio tem como objetivo fornecer um compartilhamento justo da banda passante, no qual todas as estações recebem o mesmo tratamento independentemente dos seus requisitos de QoS. Assim, redes ad-hoc que utilizam o padrão 802.11 seguem o modelo de serviço de melhor esforço, não oferecendo nenhuma garantia de QoS ao tráfego transportado. [3]

Protocolos e mecanismos específicos ao 802.11, usados em diferentes abordagens e arquiteturas, foram propostos com o objetivo de prover QoS em redes ad-hoc. No final de 2000, o grupo tarefa 802.11e iniciou o estudo e a especificação de mecanismos de suporte à QoS na subcamada MAC, seguindo a abordagem adotada pela arquitetura de diferenciação de serviços do IETF.

Alguns problemas inerentes às redes sem-fio, como o compartilhamento do meio, a necessidade de mecanismos de controle de erro nó-a-nó e os problemas de terminal escondido e exposto, dificultam a provisão de QoS nestas redes. Este artigo discute as principais questões relacionadas à provisão de QoS em redes 802.11 e fornece uma classificação das propostas de acordo com a abordagem e os mecanismos empregados.

3.8.2. Adaptadores de rede:

Os adaptadores de rede para estações podem apresentar diversas formas físicas:

- PC-Card embutidas que se encaixam nos soquetes PCMCIA, na maioria dos computadores laptop, para suplantar a blindagem interna dos computadores, as antenas e luzes de status na maioria dos adaptadores de PC-Card *wireless* se estendem cerca de 2,75 cm além da abertura do soquete na placa.
- Adaptadores de rede internos em placas PCI que se encaixam dentro de um computador desktop – A maioria dos adaptadores PCI trata-se, na realidade, de soquetes PCMCIA que permitem a um usuário conectar uma Placa de PC na parte posterior do computador. [10]
- Adaptadores USB externos – geralmente constituem uma opção melhor do que as placas de PC pois é mais fácil mover um adaptador na extremidade de um cabo para uma posição melhor.
- Adaptadores *wireless* internos embutidos em computadores laptop – são módulos conectados a placa mãe do computador.
- Adaptadores embutidos PDAs e outros dispositios handheld
- Interfaces de rede internas embutidas em outros dispositivos, com sets telefônicos compatíveis com internet e dispositivos de escritórios ou residência. [10]

Um adaptador de rede deve trabalhar com qualquer sistema operacional, desde que esteja disponível um driver para esse adaptador. Na pratica isso significa que pode encontrar drivers do Windows para quase tudo, mas terá menos opções se estiver usando um computador executanto SO Mac, Linux ou Unix. [10]

CAPITULO IV

WI-FI

O Wi-Fi é a tecnologia de conectividade sem fio mais popular no momento. Desde que foi aprovado pelo IEEE (Institute of Eletrical and Eletronics Engineers) em 1996, o padrão de rede sem fio Wi-Fi (802.11), tem crescido de forma surpreendente. Recentemente, foi divulgado que conexões sem fio já são mais populares que os antigos cabos ethernet em ambientes residenciais. O fato pode ser comprovado quando se observa que praticamente ninguém mais compra notebooks sem Wi-Fi. Muitos se referem (erroneamente) ao Wi-Fi como uma tecnologia móvel, sendo que esta, na verdade, está na categoria de tecnologias sem fio ou semi-móveis, já que a sua (semi) mobilidade existe apenas dentro dos limites da rede sem fio local. [6]

A WFA - *Wireless* Fidelity Alliance anuncia o padrão WPA - Wi-Fi Protected Access para redes *wireless* como forma de consolidar esta tecnologia junto aos usuários corporativos, que são muito sensíveis às questões de segurança.

Tecnologia Wi-Fi, também conhecida como 802.11, permite a criação de redes *wireless* num raio de até nove quilômetros. Inicialmente formada para uso doméstico, este ambiente já está sendo usado por algumas companhias para instalações em locais públicos, como aeroportos.

A ferramenta central do sistema permite que laptops e PDAs - Personal Digital Assistant configurados para esta tecnologia possam detectar automaticamente uma área de Wi-Fi e assim terem a possibilidade de se conectarem na Internet. Os usuários corporativos, no entanto, continuam cautelosos em relação à segurança destas redes, pois, dependendo da tecnologia adotada nestes ambientes, pessoas sem permissão poderiam eventualmente acessar informações confidenciais.

O Wi-Fi tem algumas variações principais:

- 802.11b, que é a mais difundida hoje, operante na faixa de frequência não regulamentada de 2.4GHz e com taxas de transferência de até 11Mbps;
- 802.11a, que opera em 5.0GHz (também não regulamentada) permite taxas de transferências bem maiores, de aproximadamente 54Mbps; [6]
- 802.11g, que também permite taxas de transferência de até 54Mpbs, porém operante em 2.4GHz.

Em termos gerais, o Wi-Fi pode ser definido como uma tecnologia de transmissão de dados via rádio ou sem fio. Temos abaixo a tabela da figura 11 com as principais características dessas três variações mais comuns.

	802.11b	802.11a	802.11g
Freqüência	2.4GHz	5GHz	2.4GHz
Taxa	11Mbps	54Mbps	54Mbps
Alcance	100-300m	30-100m	100-300m
Aplicação	A mais utilizada hoje	Aplicações específicas/estabilidade	Substituindo 11b rapidamente
Custo	Muito barata	Relativamente cara	Relativamente barata

Figura 11: Principais características das variações mais comuns.

Uma das poucas vantagens da versão 11a em relação às demais é sua estabilidade com relação às interferências: o espectro de frequência em 2.4GHz utilizado pelas versões 11b e g sofre muito com interferências causadas por alguns tipos de aparelhos domésticos, como telefones sem fio ou fornos de microondas, por exemplo. As principais desvantagens da versão 11a são o alcance reduzido (por trabalhar numa frequência mais alta, seu sinal tem mais dificuldade para se propagar em ambientes internos ou com obstáculos) e o custo relativamente mais alto que as outras versões.

A versão 11g se coloca como a mais promissora, pois é relativamente barata como a 11b e consegue taxas de transferência parecidas com as do 11a (54Mbps). Assim como o 11b, o protocolo 11g também é sensível às interferências que podem fugir do controle e do conhecimento de quem está instalando a rede. [6]

As vantagens de se ter uma rede sem fios são inúmeras: os custos para montar uma rede *wireless* são bem menores que da montagem de uma rede convencional com cabos ethernet, tendo em vista o custo de toda a infra-estrutura necessária para cabear determinado local, os custos dos próprios cabos, a mão de obra, etc.

O mercado de notebooks anda bem aquecido no que diz respeito à conectividade sem fio. Para tornar um notebook sem Wi-Fi compatível com esta tecnologia, é necessário instalar um cartão PCMCIA Wi-Fi ou algum tipo de adaptador USB. Um cartão desse tipo funciona como uma placa de rede convencional, só que sem o conector para cabo ethernet e com uma antena no lugar dele. [6]

As desvantagens de rede Wi-Fi:

• Flexibilidade: dentro da área de cobertura, uma determinada estação pode se comunicar sem nenhuma restrição. Além disso, permite que a rede alcance lugares onde os fios não poderiam chegar;

• Qualidade de serviço: a qualidade do serviço provido ainda é menor que a das redes cabeadas. Tendo como principais razões para isso a pequena banda passante devido às limitações da radiotransmissão e a alta taxa de erro devido à interferência;

• Custo: o preço dos equipamentos de Redes sem Fio é mais alto que os equivalentes em redes cabeadas;

• Segurança: intrinsecamente, os canais sem fio são mais suscetíveis a interceptores não desejados. O uso de ondas de rádio na transmissão de dados também pode interferir em outros equipamentos de alta tecnologia, como por exemplo, equipamentos utilizados em

hospitais. Além disso, equipamentos elétricos são capazes de interferir na transmissão, acarretando em perdas de dados e alta taxa de erros na transmissão.

• Baixa transferência de dados: embora a taxa de transmissão das Redes sem Fio esteja crescendo rapidamente, ela ainda é muito baixa se comparada com as redes cabeadas.

Até alguns anos, a tecnologia Wi-Fi estava presente apenas em ambientes empresariais. De lá pra cá, as vendas de roteadores sem fio, notebooks e PDAs com recursos *wireless*, bem como o número de hotspots em shoppings, aeroportos e restaurantes, têm aumentado de forma considerável. Estima-se que, em alguns anos, que o tamanho da cobertura da próxima geração de redes sem fio, o Wi-MAX, seja parecido com a da telefonia móvel, fato este que, caso se torne verdade, trará novos horizontes para o mundo das telecomunicações.

Este aspecto é da responsabilidade da WECA - *Wireless* Ethernet Compatibility Alliance, que criou a etiqueta de interoperabilidade Wi-Fi, da qual assegura a certificação e a promoção. Mesmo assim, um grande número de empresas ainda coloca actualmente a questão prática da implementação, da otimização e da segurança das redes Wi-Fi internas.

Enquanto que as vendas de interfaces rádio Wi-Fi registam uma verdadeira explosão, colocam-se algumas questões práticas na altura da implementação, da otimização e da segurança das redes Wi-Fi nas empresas.

A otimização e a implementação requerem um estudo cuidadoso da cobertura via rádio a partir dos pontos de acesso. A regulação pormenorizada da potência de emissão ou a utilização das funções específicas de equipamentos existentes no mercado permitem tirar um melhor partido da implementação.

Algumas regras simples relativas à implementação de uma rede. Em primeiro lugar, a escolha da rede sem fios tem que ser discutida. Uma das motivações pode ser o custo. Com a grande redução dos preços da tecnologia sem fios, o custo dos cabos ultrapassa geralmente o dos elementos aditivos (pontos de acesso, antena) indispensáveis a uma rede

sem fios. No entanto, existem outras razões que podem pesar na decisão, nomeadamente a mobilidade ou limitações relativamente à cabeação. [6]

Uma rede Wi-Fi implementa-se distribuindo pontos de acesso rádio. Estes são ligados a uma rede local Ethernet, que poderá manter-se independente, embora se ligue (em princípio) a outras redes - frequentemente à Internet. A regra geral que prevalece na instalação de uma rede Wi-Fi é a seguinte: os pontos de acesso têm que permitir "varrer" toda a zona de cobertura rádio desejada, minimizando ao mesmo tempo as zonas cobertas por vários pontos de acesso.

Para determinar as zonas de cobertura, é possível recorrer a uma empresa especializada, no caso de grandes implementações. Essa empresa utilizará então um analisador de espectro para estabelecer balanços de ligações. Também podemos recorrer a um portátil e a um ponto de acesso e utilizar o utilitário (existente no portátil) que fornece a potência recebida. Seguindo as indicações de sensibilidade da placa IEEE 802.11, asseguramos que o posicionamento de um ponto de acesso é conveniente e delimitamos a zona de cobertura que permite atingir. [6]

4.1 O FUNCIONAMENTO DO WI-FI

Até certo ponto, é viável lidar com as redes *wireless* como um conjunto de caixas pretas que se pode ativar e usar, sem precisar conhecer a fundo seu funcionamento. Em um mundo ideal, funcionaria dessa forma. [10]

Porém, o Ethernet *wireless* está atualmente como as transmissões por rádio estavam atualizados em 1923. A tecnologia existia, mas as pessoas gastavam muito tempo ajustando seus equipamentos e as que entediam internamente eram capazes de obter melhor desempenho de seus rádios.

Para utilizar com mais eficiência a tecnologia *wireless*, é importante entender o que acontece dentro das caixas que compõem a rede. Este tópico descreve padrões e especificações que controlam as redes *wireless*, explicando também como os dados são transportados através da rede de um computador para outro. O transporte de dados através de uma rede *wireless* envolve três elementos distintos: os sinais de rádio, o formato dos dados e a estrutura da rede. Cada um desses elementos é independente dos outros dois; portanto, é necessário definir todos os três quando se define uma nova rede. No que se refere ao modelo OSI, o sinal de rádio opera na camada Física, enquanto o formato dos dados controla várias das camadas mais elevadas. A estrutura de rede inclui os adaptadores de interface e as estações base, os quais enviam e recebem os sinais de rádio. [10]

Em uma rede *wireless*, os adaptadores de rede em cada computador convertem os dados digitais para sinais de rádio, os quais são transmitidos para outros dispositivos na rede, e convertem os sinais de rádio que chegam a dados digitais. O IEEE (*Institute Electrical and Electronics Engineers*) produziu um conjunto de padrões e especificações para redes *wireless*, sob o título "IEEE 802.11", o qual define o formato e a estrutura dos sinais.

4.1.1 Sinais de rádio

As redes 802.11b operam em uma banda especial de frequência em torno dos 2,4 GHz, a qual foi reservada, na maior parte do mundo, para serviços de rádio ponto-a-ponto de espalhamento de espectro não licenciado. Teoricamente, a tecnologia de espalhamento de espectro possibilita a coexistência com outros usuários (até certo ponto), sem uma interferência significativa.

Um serviço de rádio ponto-a-ponto opera um canal de comunicação que transporta informações de um transmissor até um único receptor. O contrário de um ponto-a-ponto é o serviço de radiodifusão, que envia o mesmo sinal para muitos receptores ao mesmo tempo.

Espalhamento de espectro é uma família de métodos para a transmissão de um único sinal de rádio, usando um segmento relativamente amplo do espectro de rádio. As WLANs usam dois sistemas de transmissão de rádio diferentes: FHSS (*Frequency-Hopping Spread Spectrum*) e DSSS (*Direct-Sequence Spread Spectrum*). Algumas redes 802.11 mais antigas usam o sistema FHSS mais lento, mas a geração atual das WLANs usam o DSSS. O espalhamento de espectro oferece algumas vantagens importantes sobre outros tipos de sinais de rádio que usam um único canal menos amplo. O espalhamento de espectro é extremamente eficiente; portanto, os transmissores de rádio podem operar com muito pouca energia. Por operarem em uma banda relativamente ampla de freqüências, são menos sensíveis a interferência de outros sinais de rádio e ruídos elétricos, o que significa que os sinais geralmente são capazes de ter acesso a ambientes onde um sinal de banda estreita convencional não poderia ser recebido ou entendido, e devido a uma determinada freqüência deslocar-se entre múltiplos canais, podendo ser extremamente difícil para um sintonizador, o que não autorizado interceptar e decodificar o conteúdo de um sinal. [10]

4.1.1.1 Frequency-Hopping Spread Spectrum (FHSS)

O projeto original de Lamarr e Antheil para o rádio de espalhamento de espectro usava um sistema de salto de frequência. Como sugere o nome, a tecnologia FHSS divide um sinal de rádio em pequenos segmentos e "salta" de uma frequência para outra várias vezes por segundo, à medida que transmite aqueles segmentos. O transmissor e o receptor estabelecem um padrão de saltos sincronizados que definem a ordem de seqüência na qual serão usados diferentes canais. [10]

4.1.1.2 Direct-Sequence Spread Spectrum (DSSS)

A tecnologia DSSS usa um método conhecido como seqüência 11-chip Barker para espalhar o sinal de rádio através de um único canal com 22 MHz de largura, sem alterar as

frequências. Cada link do DSSS utiliza um único canal, sem qualquer salto entre as frequências. Como mostra a Fig. 12, a transmissão DSSS usa mais largura de banda, mas energia menor em comparação a um sinal convencional. O sinal digital à esquerda representa uma transmissão convencional na qual a energia é concentrada dentro de uma largura de banda mais compacta. O sinal do DSSS à direita utiliza a mesma quantidade de energia, mas a espalha através de uma banda mais ampla de freqüências de rádio. [10]

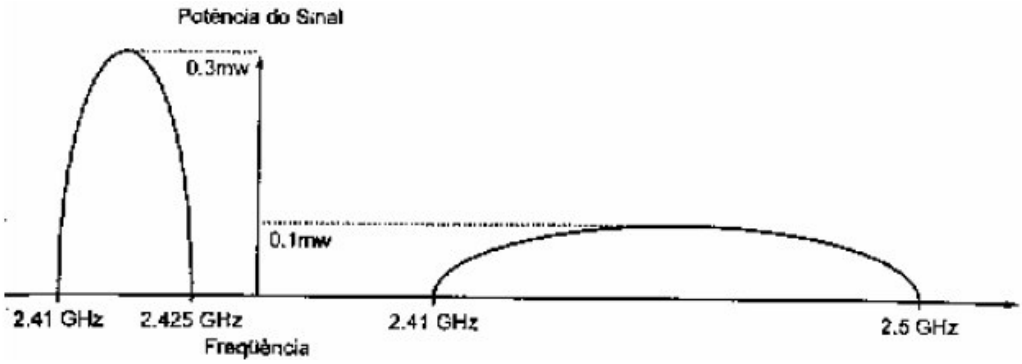

Figura 12: Sinais de rádios convencionais e DSSS

Evidentemente, o canal DSSS de 22 MHz é um pouco mais extenso do que os canais de 1 MHz usados no sistema FHSS. Um transmissor DSSS quebra cada pedaço do fluxo de dados original em uma série de padrões de bits redundantes denominados chips, e os transmite para um receptor que reagrupa os chips de volta em um fluxo de dados idêntico ao original. A maior parte da interferência provavelmente ocupa uma largura de banda mais estreita do que um sinal DSSS e, além disso, cada bit é dividido em diversos chips; portanto, o receptor geralmente pode identificar ruídos e rejeitá-los, antes de decodificar o sinal. Da mesma maneira que outros protocolos de rede, um link DSSS *wireless* troca mensagens de estabelecimento de comunicação dentro de cada pacote de dados para confirmar se o receptor consegue entender cada pacote. [10]

4.2 VERIFICAÇÃO DE ERROS

Em um circuito de transmissão ideal, o sinal observado em uma extremidade é absolutamente idêntico ao que surge na outra extremidade. Porém, no mundo real, quase sempre haverá algum tipo de ruído capaz de interferir com o sinal original. Ruído é definido como qualquer coisa que seja adicionado ao sinal original. Qualquer que seja a causa, o ruído no canal é capaz de interromper o fluxo de dados. Em um sistema de comunicações moderno, esses bits são transportados com extrema rapidez de forma que um ruído que ocorra por uma fração de segundo pode comprometer seriamente a comunicação. [10]

Sendo assim, deve-se inserir um processo conhecido como verificação de erros no fluxo de dados. A verificação de erros é obtida pela inclusão de algum tipo de informação padronizada, conhecida como *checksum*, em cada byte. Se o checksum apurado pelo receptor não for o esperado é solicitada uma retransmissão.

4.3 Controles de rede *wireless* 802.11b

A especificação 802.11b controla a maneira como os dados são transportados através da camada física (o link do rádio), definindo uma camada Media Access Control (MAC) que manipula a interface entre a camada física e o restante da estrutura da rede.

4.3.1 A camada física

Em uma rede 802.11, o transmissor adiciona um preâmbulo de 144 bits a cada pacote, sendo 128 bits, utilizados pelo receptor para se sincronizar com o transmissor, e um campo start-of-frame de 16 bits. Isso tudo é seguido por um campo de 48 bits, contendo informações sobre a velocidade de transferência dos dados, o comprimento dos dados

contidos no pacote e uma seqüência de verificação de erros. Esse cabeçalho é conhecido como preâmbulo PHY, pois controla a camada física do link de comunicações. O cabeçalho especifica a velocidade dos dados que o seguem; portanto, o preâmbulo e o cabeçalho sempre são transmitidos em 1 Mbps. Assim, mesmo que um link esteja operando em 11 Mbps pleno, a velocidade efetiva será consideravelmente mais lenta. Na prática, pode-se esperar, no máximo, 85 por cento da velocidade nominal. Esse preâmbulo de 144 bits é remanescente dos sistemas DSSS mais antigos e lentos, tendo permanecido na especificação para garantir a compatibilidade dos dispositivos 802.11b com os padrões mais antigos, mas na prática, ele não faz nada de útil. Existe uma alternativa opcional que usa um preâmbulo de 72 bits, mais curto. Em um preâmbulo mais curto, o campo de sincronização possui 56 bits combinados com o mesmo campo start-of-frame de 16 bits, usado em preâmbulos longos. O preâmbulo curto é incompatível com os hardware 802.11 antigo. Uma rede leva o máximo de 192 milisegundos para manipular um preâmbulo longo, se comparado aos 96 milisegundos para um preâmbulo curto. O que constitui uma significativa diferença entre o preâmbulo curto, no que se refere ao throughput (quantidade de dados transmitidos em uma unidade de tempo) de dados real, especialmente para fatos como fluxo de serviços de áudio, vídeo e de voz na Internet.

Alguns fabricantes usam o preâmbulo como padrão, enquanto outros usam o preâmbulo curto. Geralmente, é possível alterar o comprimento do preâmbulo no software de configuração de adaptadores de rede e pontos de acesso (AP – Access Point).

4.3.2 A camada MAC

A camada MAC controla o tráfego que ocorre na rede de rádio, evitando as colisões e os conflitos de dados, ao usar um conjunto de regras denominado *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA), e suportando as funções de segurança especificadas no padrão 802.11b. Quando a rede inclui mais de um AP, a camada MAC, associa cada cliente de rede com o AP que proporciona a melhor qualidade de sinal. [10]

Quando mais de um nó na rede tenta transmitir dados no mesmo instante, o CSMA/CA instrui todos os nós conflitantes, para recuar e tentar novamente mais tarde, e permite que o nó sobrevivente envie seu pacote.

O CSMA/CA também possui um recurso opcional que define um AP como um ponto coordenador, capaz de conceder a prioridade para um nó de rede que esteja tentando enviar tipos de dados críticos com relação ao tempo, como de voz ou streaming *media*.

A camada MAC pode suportar dois tipos de autenticação para confirmar se um dispositivo de rede está autorizado a se associar à rede: autenticação aberta e autenticação de chave compartilhada. Quando se configura a rede, todos os nós na rede devem usar o mesmo tipo de autenticação. [10]

A camada MAC também define diversas opções no adaptador de rede:

- Power mode – o adaptador de rede suporta dois modos de energia: *Continuous Aware Mode* e *Power Save Polling Mode*. No primeiro, o receptor de rádio sempre estará ligado e consumindo energia. No *Power Save Polling Mode*, o rádio está ocioso na maior parte do tempo, mas efetua sondagens periódicas ao AP em busca de novas mensagens.

- Access Control – o adaptador de rede contém o controle de acesso que mantém os usuários não autorizados longe da rede. Uma rede 802.11b pode usar duas formas de controle de acesso: o SSID (*Service Set Identification*) (o nome da rede) e o endereço MAC (uma string de caracteres única, identificando cada nó da rede). Cada nó na rede deve ter o SSID programado nele, ou o AP não se associará com aquele nó. Uma tabela opcional de endereços MAC pode restringir o acesso aos rádios cujos endereços estejam na lista.

- WEP encryption – o adaptador de rede controla a função de criptografia *Wired Equivalent Privacy* (WEP). A rede pode usar uma chave de criptografia de 64 ou 128 bits, para codificar ou decodificar dados.

4.3.3 *Wireless*

Esta etapa identifica os elementos que compõem uma rede *wireless*, oferecendo também conselhos para ajudar a decidir quais componentes melhor atenderão a necessidades específicas.

4.4 ADAPTADORES DE REDE

Um adaptador de rede é a interface entre um computador e uma rede. Em uma rede *wireless*, o adaptador contém um transmissor de rádio que envia os dados do computador para a rede, e um receptor que detecta os sinais que chegam e os passa para o computador. Deve-se considerar vários aspectos ao selecionar um adaptador de interface: o pacote físico, o tipo de antena, a compatibilidade com os pontos de acesso e outros nós da rede, e a compatibilidade com o sistema operacional do computador. [10]

4.4.1 PC-Card

Adaptadores de rede em PC-Card são o tipo mais popular, pois a utilização mais freqüente é a adição de computadores portáteis a LANs existentes. Praticamente todos os fabricantes de padrão 802.11b possuem, pelo menos, um adaptador de PC-Card em sua linha de produtos. Os adaptadores são compactos e leves.

Todos os adaptadores PC-Card têm uma aparência bastante parecida, pois todos precisam se encaixar no soquete PCMCIA do computador. Eles têm o tamanho aproximado de um cartão de crédito, com um conector em uma ponta e, na outra, uma cobertura de plástico para a antena interna ou um conector para uma antena externa. A maioria dos adaptadores PC-Card inclui uma ou duas luzes indicadoras na seção externa ao computador. Uma luz

que indica se o adaptador está recendo energia do computador e o outro se acende quando o adaptador detecta um link de rádio ativo de um outro dispositivo.

Muitos adaptadores contêm duas antenas internas com uma diversidade de sistemas que comparam constantemente a qualidade dos sinais que chegam às antenas e seleciona automaticamente o mais forte. Embora as duas antenas estejam apenas três a cinco centímetros separadas uma da outra, a melhoria proporcionada pode ser marcante. Os adaptadores PC-Card geralmente possuem antenas omnidirecionais embutidas mas alguns fabricantes também oferecem versões com conectores para antenas externas. A opção entre a interna e a externa é sempre difícil. Porém, é bom salientar que as antenas externas podem ser unidirecionais o que melhora consideravelmente sua performance. [10]

4.4.2 Adaptadores USB

Caso o computador possua uma porta USB (*Universal Serial Bus*), uma adaptador USB *wireless* poderia ser a melhor maneira de conectar esse computador à rede 802.11b. O adaptador se conecta através de um cabo; portanto, nunca é um problema mover o adaptador inteiro para uma melhor posição. A maioria dos adaptadores USB possui antenas cativas, geralmente montadas em articulações ou suportes que permitem promover ajustes finos em suas posições. As antenas também costumam ser maiores e mais fáceis de manipular neste padrão. Assim, pode-se esperar uma melhor qualidade de sinal em um dispositivo USB. [10]

4.4.3 Placas de expansão internas

Os adaptadores *wireless* internos mais comuns são, na realidade, PC-Card montadas em soquetes PCMCIA que se encaixam em um slot de expansão PCI ou ISA. Porém, esta solução tem uma série de desvantagens, principalmente, na questão de interferências e posicionamento para obtenção de um melhor sinal. Se houver problemas, existem duas

maneiras de lidar com isso. Uma, seria usar um adaptador que possuísse conector para a instalação de antena externa. E a outra, seria a utilização de um adaptador USB pois, caso o computador não tivesse esse tipo de porta, há a possibilidade de se adicioná-la em placas de expansão PCI ou ISA.

4.4.4 Adaptadores internos

Diversas marcas importantes de notebooks começaram a apresentar adaptadores de rede *wireless* on-board. A vantagem óbvia é que o adaptador interno não exige transporte e já vem configurado. Se for esse o caso, é bom certificar-se de ter uma maneira fácil de desativar o adaptador quando não estiver em uso.

4.4.5 Compatibilidade de sistema operacional

Da mesma maneira que qualquer outro dispositivo que seja usado com o computador, um adaptador de rede *wireless* exige um driver específico que contenha controles e interfaces que permitam ao adaptador trocar dados com o computador. Normalmente, esses drivers deverão acompanhar o equipamento. Caso contrário, será necessário encontrá-lo em algum outro lugar (site do fabricante, por exemplo) ou escolher um adaptador diferente que suporte seu sistema operacional.

4.4.6 Facilidade de utilização do programa

Cada adaptador *wireless* usa um programa utilitário de configuração que controla o modo de operação, o número do canal e todas as outras opções de configuração que devem combinar com as configurações para os outros nós da rede. O fabricante geralmente fornece o programa em um CD ou disquete que vem junto com o adaptador.
Em condições ideais, um usuário comum nunca precisaria examinar o utilitário de configuração. Mas, eventualmente, se faz necessário modificar tais parâmetros. Portanto,

tanto o utilitário de configuração quanto o display de status devem ser de fácil entendimento e utilização.

4.5 SEGURANÇA

A especificação 802.11b inclui um esquema de segurança denominado WEP que usa uma chave de criptografia de 64 ou 128 bits. O formato de 64 bits é um padrão comum mas existem algumas diferenças entre as técnicas de criptografia de 128 bits oferecidas por diversos fabricantes. Portanto, nem sempre é possível que diferentes marcas de adaptadores e pontos de acesso troquem dados, quando seus recursos de segurança aprimorada estão ativos. Se a segurança aprimorada for indispensável, poderá ser necessário adotar uma padronização, por uma única marca de hardware ou por um grupo de marcas que compartilhem o mesmo tipo de criptografia de 128 bits (como Cisco, como mostrado na figura 13 e Xircom como mostrado na figura 14 ou Orinoco e AirPort da Apple). [10]

Figura 13: **Cisco** Aironet 340 Series PC-Card

Figura 14: Xircom

4.6 DOCUMENTAÇÃO E SUPORTE TÉCNICO

Todos os fabricantes de hardware Ethernet *wireless* oferecem algum tipo de suporte técnico para seus usuários. Entretanto, a qualidade e a utilidade do suporte variam amplamente de um fornecedor para outro. No mínimo, um nível adequado de suporte técnico deve incluir um manual de usuário preciso e escrito com clareza, um centro de suporte que responda a perguntas específicas por telefone e e-mail, um site com respostas a perguntas freqüentes e um centro de download que ofereça as versões mais recentes dos drivers de dispositivo, os utilitários de configuração, e software de display de status, disponíveis para download gratuito. [10]

4.7 ADAPTADORES PARA REDES AD-HOC

Em uma rede Ad-Hoc, cada adaptador de rede troca dados com todos os demais nós por meio de links diretos, sem um AP atuando como um nó central. As redes Ad-Hoc são úteis para redes isoladas e de pequeno porte, e compartilhamento de arquivos ponto-a-ponto direto. Por exemplo, alguém que usar um notebook e um computador desktop, pode configurar uma rede Ad-Hoc para transferir arquivos entre os dois. As redes Ad-Hoc *wireless* são bem menos comuns do que redes de infra-estrutura, mas fazem parte da especificação 802.11b; portanto, quase todas as interfaces de adaptador de rede *wireless* e programas de configuração oferecem uma opção para rede Ad-Hoc. Segue um exemplo na figura 15.

Figura 15: Exemplo de uma **rede Ad-hoc**

4.8 ADAPTADORES DE DUPLA FINALIDADE

As redes Wi-Fi tornaram-se amplamente populares mas não se trata da única tecnologia disponível. Também estão disponíveis diversos outros sistemas, incluindo Bluetooth (que proporciona conexões com intervalo muito curto para dispositivos periféricos e acessórios para computadores, como headfones e teclados) e 802.11a (que usa um conjunto diferente de frequências de rádio para proporcionar um link de velocidade mais elevada com uma rede, do que a 802.11b). Cada uma dessas opções oferecem soluções, até certo ponto, para um conjunto diferente de problemas, e cada uma atende um nicho de mercado específico. Vários fabricantes anunciaram novos produtos que combinam uma interface de adaptador de rede 802.11b com uma interface com algum outro serviço *wireless*. Alguns podem detectar e utilizar tanto redes 802.11b (2.4 GHz) quanto 802.11a (5.4 GHz), enquanto outros integram redes 802.11b com o Bluetooth.[10]

Um adaptador de rede dupla finalidade ideal detectaria automaticamente os sinais de rádio de todas as redes compatíveis, dentro de um intervalo, e permitiria que um usuário configurasse uma conexão instantânea com qualquer uma dessas redes, sem a necessidade de se preocupar com o tipo de link que está sendo usado pela rede. É possível que esse adaptador de rede *wireless* surja nos próximos anos. Por exemplo, no início de 2002 foi introduzida a Blue802 pela Intersil e a Silicon Wave. A Blue802 permite que conexões Bluetooth e 802.11b operem simultaneamente por meio de um único adaptador; dessa forma, um computador pode usar links Bluetooth para um mousar, um teclado, uma impressora ou outro computador no mesmo instante em que está conectado à Internet ou a uma LAN através da rede Wi-Fi. Isso é um grande negócio, pois tanto o 802.11b quanto o Bluetooth usam as mesmas frequências de rádio (2.4 GHz) e cada serviço geralmente pode causar interferências nos outros. O Blue802 coordena os dois tipos de transmissão de rádio a fim de aperfeiçoar o desempenho de ambos. Segue com a figura 16.

Figura 16 Belkin Flip é um **adaptador**

4.9 PONTOS DE ACESSO

A maioria dos adaptadores de rede têm uma única função: trocar dados entre um computador e uma rede. Os pontos de acesso, por outro lado, oferecem uma ampla variedade de recursos e funções. Eles estão disponíveis como pontos de acesso simples em combinação com hubs, switches e roteadores para conexões com fio, computadores e outros dispositivos próximos. Existe uma categoria completa de pontos de acesso *wireless* para redes domésticas, denominada gateways residenciais. [10]

4.9.1 LANs *wireless* puras

Quando todos os nós em uma LAN trocam dados por rádio, o ponto de acesso atua como um hub que proporciona o ponto de controle central para a rede. Na verdade, o "ponto de acesso" nesse tipo de rede não proporciona acesso a coisa nenhuma, exceto a outros nós *wireless*. Esse tipo de arranjo *wireless* constitui uma das funções básicas de qualquer AP;

portanto, se for esse o projeto, deve-se usar um modelo mais simples e mais barato que seja capaz de proporcionar um sinal útil para sua área de cobertura.

4.9.2 Múltiplos pontos de acesso

Um único AP pode ser completamente adequado para suportar uma WLAN em um espaço aberto e relativamente pequeno, com um volume moderado de tráfego. Porém, quando a rede precisar cobrir uma área muito ampla, ou um espaço com obstruções causadas por paredes, mobílias ou outros objetos, ou por interferência de outros rádios, provavelmente se precisará adicionais mais pontos de acesso. [10]

A maioria das redes domésticas, e muitas redes em pontos comerciais muito pequenos, precisa de um único AP; portanto, a escolha de um AP que suporte roaming caracteriza um problema para os gerentes de redes extensas e complexas. A especificação 802.11b inclui uma função roaming que muda de AP quando a qualidade de sinal do novo AP é melhor que o original. Depois de se associar a um novo AP, ele inspeciona todos os outros canais de rádio a fim de determinar se algum outro AP, operando em um canal diferente, oferece um serviço melhor. Caso encontre, a troca se efetua novamente.

Múltiplos pontos de acesso em uma LAN com fio permitem que usuários *wireless* possam se utilizar desse serviço. Na maioria dos casos, um cliente de rede não se associará a um AP diferente, a menos que o cliente se mova para um local diferente enquanto o link com a rede está ativo ou quando ocorre o aumento do volume de tráfego no canal atual.

Na maioria das situações, múltiplos pontos de acesso devem ser posicionados de forma a proporcionar uma cobertura que sobreponha em cerca de 30 por cento um AP para o próximo. Entretanto, se a WLAN precisar suportar uma grande quantidade de usuários simultâneos, a melhor maneira de promover o balanceamento de carga consistirá em instalar dois ou mais pontos de acesso no mesmo local, com cada AP definido com um canal de rádio diferente e não-interferente.

4.10 ANTENAS EXTERNAS

Se consegue estabelecer um link de dados confiável de alta velocidade com qualquer local da rede, usando as antenas embutidas nos adaptadores e pontos de acesso, certamente não haverá motivo para desperdiçar tempo, dinheiro ou energia, com antenas externas.

Mas quando as condições de recepção não forem perfeitas, ou quando se quer enviar um sinal de rádio o mais distante possível, uma antena separada poderá evitar a interferência, aumentar a velocidade de transferência dos dados, expandir a área de cobertura e estabelecer links de comunicação confiáveis em locais onde seriam pouco mais que um "ruído" com antenas internas comuns.

Só para referência, uma antena externa onidirecional amplia a área de sinal útil para cerca de 35 metros de distância, ao invés dos 10 metros para antenas embutidas. Usando-se antenas externas nas duas extremidades, pode-se esperar um alcance de 40 metros. A forma da área de cobertura da antena direcional e sua quantidade de ganho (força do sinal do transmissor e sensitividade do receptor) dependem do desenho exato de cada antena. Algumas antenas direcionais podem proporcionar uma quantidade moderada de ganho com relação a um padrão mais amplo, enquanto outras podem focalizar três ou quatro vezes (ou ainda mais), e o ganho se dará em uma área muito mais restrita. [10]

Antenas direcionais podem proporcionar uma enorme melhoria na qualidade do sinal sobre uma área de cobertura firmemente focalizada, podendo também reduzir a interferência de áreas "nulas" fora daquele padrão de cobertura, o que significa que podem apresentar diversas utilizações em uma WLAN:

- Podem permitir que um usuário fora da área "normal" de cobertura se associe à rede;
- Podem aumentar a área de cobertura efetiva, servida por um AP, limitando a cobertura a uma direção;
- Podem reduzir ou eliminar o efeito da interferência off-axis de outros sinais de rádio;
- Podem reduzir a quantidade de interferência que uma WLAN cria para outros rádios;

- Podem estabelecer links ponto-a-ponto de longa distância e estacionários entre prédios.

4.10.1 Características da antena

As antenas externas apresentam formas e tamanhos variados. Ao selecionar uma antena, deve-se considerar vários itens, incluindo o padrão de cobertura, o ganho, o fator de formação e a resistência às intempéries. [10]

4.10.2 Padrão de cobertura

A folha de especificação de uma antena inclui um diagrama mostrando a forma do padrão de cobertura da antena. De modo geral, o padrão é onidirecional (irradia e recebe igualmente bem em todas as direções), direcional (com a radiação ou recepção mais forte em uma direção) ou figureeight (boa cobertura para a parte frontal e posterior e cobertura fraca nas laterais).

Os catálogos e as folhas de especificação para antenas direcionais geralmente incluem um ângulo de abertura, largura do feixe, ou área de captura, expressos em graus. O ângulo de abertura é a seção de um círculo que contém a cobertura ou sensitividade de energia máxima da antena. Por exemplo, se uma antena tiver um ângulo de abertura de 45 graus, a cobertura ou sensitividade máxima se estenderá para fora da parte frontal da antena, em um ângulo de 45 graus.

4.10.3 Ganho

O ganho de uma antena é a proporção entre a energia da transmissão ou da sensitividade da recepção, quando comparada a uma antena bipolar padrão (um bipolo é uma antena direta, alimentada pelo centro, com metade do comprimento de onda, como a antena *twin-lead* em

forma de T, fornecida com muitos rádios e sintonizadores de FM). O ganho geralmente é expresso em dB*i* (decibéis over isotrópico).

4.10.4 Fator de formação

Uma antena bipolar para um rádio com 2.4 GHz tem somente cerca de 2,75 cm de comprimento, mas os refletores e outros elementos que adicionam ganho e características direcionais podem ser muito mais longos.

As antenas omnidirecionais são sempre cabos ou hastes verticais. Algumas antenas omnidirecionais de alto ganho podem ter até 60 ou 90 centímetros de comprimento. Para a utilização em ambientes fechados, especialmente em ambientes com tetos rebaixados, antenas omnidirecionais especiais montadas no teto, podem constituir uma excelente opção para uma rede *wireless*.

As antenas direcionais podem apresentar várias formas, incluindo pratos e painéis parabólicos que incluem um refletor atrás da parte ativa da antena; as antenas que se assemelham a uma versão mais curta de uma antena de TV de telhado; e antenas *patch* ou de painel com diversos elementos. [10]

4.11 INSTALAÇÃO E CONFIGURAÇÃO DOS PONTOS DE ACESSO

Quando decide começar a usar uma WLAN, tem pelo menos duas opções: pode desempacotar todas as caixas, conectar os rádios aos computadores e tentar fazer tudo isso funcionar; ou fazer algum planejamento avançado e pensar sobre o melhor local para cada componente.

4.11.1 Quantos pontos de acesso?

Uma rede *wireless* simples opera com um único AP e vários nós de rede. Entretanto, quando estiver tentando cobrir um espaço amplo, provavelmente precisará de pelo menos um ponto adicional.

Quando precisa de mais de dois pontos de acesso em um espaço complexo, deve começar a cogitar a utilização de uma combinação de antenas omnidirecionais e direcionais, em vez das omnidirecionais embutidas em alguns pontos de acesso. Uma sugestão seria cortar alguns círculos que cubram o equivalente a 45 ou 60 metros, e outros que combinem com o padrão de antenas direcionais, e movê-los até encontrar uma combinação de locais que proporcione a máxima cobertura.

A quantidade de pessoas que utiliza a rede também pode apresentar um efeito sobre a quantidade de pontos de acesso necessários. Como um limite prático, se mais de meia dúzia de computadores estiverem tentando se conectar ao mesmo AP no mesmo instante haverá uma queda no desempenho da rede.

Se a quantidade de usuários aumentar ao longo do tempo, pode descobrir que a performance se deteriora devido aos pontos de acesso estarem operando em plena capacidade, ou próximo a ela. Quando isso ocorre, hora de pensar na adição de mais pontos de acesso. Sempre que possível, definir os novos pontos de acesso com uma quantidade de canais diferentes e não interferentes e reconfigurar metade dos nós da rede para que utilizem esse canal. [10]

Ao operar no modo de infra-estrutura, cada nó se comunica com a rede através de um AP. Portanto, não é necessário que todos os nós estejam usando o mesmo número de canal. Se puder distribuir seus nós entre dois ou três canais não interferentes, reduzir a quantidade de links em cada canal, o que melhorará o desempenho para toda a rede.

4.11.2 Problemas de interferência

Se não houver nenhum usuário usando uma WLAN ou outro dispositivo de 2.4 GHz a, aproximadamente, 800 metros de distância, não precisa se preocupar com interferência na rede. Isso está se tornando pouco provável a cada dia. Outros serviços de rede, junto com os telefones sem fio, fornos de microondas, sistemas de iluminação externa e brinquedos controlados por rádio, usam o mesmo conjunto de frequências.

Se existir muita interferência de rádio ao seu redor, provavelmente descobrirá isso durante a sondagem do local. Pode fazer duas tentativas para reduzir ou eliminar a interferência: remover a fonte de interferência ou mover a rede para um canal diferente. A alteração dos canais geralmente é a mais fácil, mas nem sempre é eficiente, pois a fonte de interferência pode ser uma frequência de rádio que salta através da banda de 2.4 GHz.

Para tentar eliminar a interferência siga os seguintes passos, na ordem:

1. Transferir para um canal diferente pelo menos cinco números distante daquele no qual se encontrou o problema.

2. Descubrir se existe um telefone sem fio, um forno de microondas ou algum outro dispositivo que opere a 2.4 GHz. Se possível, substituir o dispositivo por outro que opere em uma frequência diferente, como um telefone sem fio de 900 MHz.

3. Se puder alterar a potência de saída dos rádios nos seus pontos de acesso e adaptadores de interface, certifique-se se estão definidos com a configuração alta (geralmente 100 mW).

4. Verifique com vizinhos se eles estão usando uma rede *wireless*.

5. Substitua as antenas omnidirecionais por direcionais, a fim de aumentar a força do sinal e a sensitividade dos receptores. Talvez você precise mudar o ponto de acesso para outro local, ou adicionar mais pontos de acesso, para cobrir a mesma área.

Após isso, não tem muito que fazer, exceto se conformar com uma fraca performance ou substituir a sua rede Wi-Fi de 2.4 GHz por uma rede *wireless* 802.11a que opere a 5.2 GHz. Pode encontrar outra fonte de interferência, mas ela provavelmente não ficará evidente até que sua rede tenha sido colocada em operação por algum tempo.

4.11.3 Instalando pontos de acesso

Como já citado, muitos pontos de acesso são combinados com outros dispositivos, como roteadores de rede, roteadores de Internet de banda larga e HUBS de Ethernet tradicionais. No mínimo, cada ponto de acesso deve incluir um transmissor e um receptor de rádio, uma ou duas antenas cativas ou conectores para antenas externas, e uma porta Ethernet para conectar a uma rede com fio. O ponto de acesso também deve possuir algum tipo de software de configuração interno que exiba as configurações atuais e aceite comandos para a efetivação de alterações. [10]

Devido ao fato de cada ponto de acesso acompanhar um pacote diferente com diferentes inputs, outputs e controles, deve seguir as instruções de instalação e configuração específicas, fornecidas com o próprio dispositivo. Infelizmente, os manuais dos fabricantes nem sempre proporcionam todas as informações necessárias.

4.11.4 Comandos de configuração e definições

Cada utilitário de configuração manipula comandos de configuração e definições de diferentes maneiras, mas cada ponto de acesso, que obedece às especificações da 802.11b, deve incluir o mesmo conjunto básico de opções. Ao configurar a rede, provavelmente desejará alterar algumas dessa opções, a partir dos valores padrão.

Em geral, o utilitário de configuração deve incluir as opções: endereço IP, máscara de sub-rede, ID de rede *wireless*, canal, segurança e DHCP.

4.11.4.1 Endereço IP

Este campo exibe o endereço IP numérico usado atualmente pelo ponto de acesso. Este pode ser um endereço padrão atribuído na fábrica, um endereço atribuído pelo gerente da rede ou um endereço atribuído pelo servidor de DHCP.

4.11.4.2 Máscara de sub-rede

Este campo identifica a sub-rede que inclui o ponto de acesso e os clientes *wireless* que se conectam à *LAN* por meio do ponto de acesso. O endereço da *sub-rede* é atribuído pelo gerente da rede.

4.11.4.3 Canal

A configuração do canal equivale ao número do canal de rádio que será usado pelo AP para trocar dados com o dispositivo cliente na WLAN. Cada AP opera em um canal único, mas a maioria dos adaptadores varre os canais para encontrar o melhor sinal disponível com o mesmo SSID. Caso tente usar um adaptador com um canal predefinido, esse número de canal terá que combinar com o do AP. [10]

Se a rede incluir mais de um AP, deve definir pontos de acesso adjacentes a canais diferentes conforme já visto anteriormente.

4.11.4.4 Segurança

O WEP é o sistema de segurança que supostamente mantém as pessoas que não tenham o código-chave eletrônico apropriado, afastadas da sua rede. Todos os componentes de hardware 802.11b vêm acompanhados com a criptografia WEP opcional; portanto deve saber como usá-la.

Geralmente, é mais fácil configurar uma WLAN com a criptografia desativada mas é uma idéia muito boa ativá-la quando começar a trafegar dados reais através da rede. [10]

4.11.4.5 DHCP

Um ponto de acesso pode atuar como servidor de DHCP, porém somente um servidor DHCP pode estar ativo em qualquer momento; portanto, se a rede já tem um servidor DHCP ativo, desativar essa função do AP.

Quando o servidor de DHCP do ponto de acesso estiver ativo, o utilitário de configuração deverá exibir uma lista de clientes DHCP atualmente ativos na mesma tela que contém as opções ativar/desativar *(enable/disabl*e), ou o utilitário pode se oferecer para abrir outra janela com os dados.

4.11.5 Múltiplos pontos de acesso

Muitas redes usam mais de um AP para ampliar a cobertura da rede além do sinal de uma única estação base.

No caso do cliente da rede se movimentar ocorre o roaming. A especificação 802.11b possibilita que o cliente se mova de um AP para outro, mas não define o processo de troca (hand-off). Nesse caso, cada fabricante de AP lançou seu próprio método, que pode não ser compatível com nenhum outro. Isso provavelmente será alterado num futuro próximo mas, no momento, é de fundamental importância usar apenas um tipo de AP na rede. Pode-se esperar que um adaptador Wi-Fi trabalhe com qualquer tipo de AP, mas não é seguro que dois tipos diferentes de pontos de acesso funcionem em conjunto. [10]

Para configurar uma WLAN com mais de um ponto de acesso, simplesmente conectar todos os pontos à mesma rede Ethernet com fio e configurar para que manipulem as mesmas chaves SSID e WEP. Se não usar um servidor de DHCP, atribuir um endereço IP diferente para cada um dos APs, mas utilizar a mesma sub-rede e gateway para a rede inteira. Se um AP estiver atuando como servidor de DHCP, lembrar de desativar a função de DHCP em todos os outros APs da rede.

CONCLUSÃO

O Wi-Fi é a tecnologia de conectividade sem fio no momento mais popular. Foram feitas várias pesquisas com o Wi-Fi, também conhecido como 802.11, e com isso se encontram algumas variações, assim como a 802.11a, 802.11b, 802.11g. As redes 802.11 podem ser utilizadas para complementar as redes celulares de terceira geração.

Com relação a segurança das redes wireless, o assunto é tratado ainda de forma muito delicada, tanto pelos que utilizam a tecnologia, quanto pelos fabricantes de equipamentos. Segurança, apesar de ser um item fundamental em qualquer projeto de rede, tem sido tratado com certo descaso pelas pessoas que estão montando uma pequena rede.

Por se tratar de uma tecnologia relativamente barata e de fácil instalação, o seu uso tem grandes perspectivas de continuar crescendo, pois um de seus melhores atrativos é a mobilidade.

Existem estudos e implementações avançados em redes de nova geração, convergência de rede, mobilidade, IPV6, etc, que certamente farão uso dessa mobilidade total e não somente dentro da área da WLAN.

Como proposta para estudos futuros o estudo das implementações, criação de Manual, testes com placas de redes, e também uma proposta para o desenvolvimento de uma ferramenta que consiga descobrir uma forma para que os equipamentos elétricos não sejam capazes de interferir nas transmissões, acarretando em perdas de dados e alta taxa de erros na transmissão. Baixa transferência de dados: embora a taxa de transmissão das Redes sem Fio esteja crescendo rapidamente, ela ainda é muito baixa se comparada com as redes cabeadas.

REFERENCIA BIBLIOGRAFICA

[1] – CABIANCA, Luís Antonio; BULHMAN, Haroldo José *"Redes LAN / MAN Wireless I: Padrões 802.11 a, b, e g"*, Tutorial, On–line: http://www.teleco.com.br/ tutoriais/tutorialrwlanman1/default.asp.

[2] – Wikipédia, a enciclopédia livre, *"IEEE – Instituto de Engenheiros Eletricistas e Eletrônicos"*, On–line: http://pt.wikipedia.org/wiki/Instituto_de_Engenheiros_ Eletricistas_e_Eletrônicos, 20/05/2007.

[3] CAMPES, Floriano. Entenda o que Wireless Lan (Apostila). (2005).

[4] JUNIOR, Nilton Alves; SILVA, Sandro Luiz P. - Introdução as Redes Wireless, (2006), **Editora** UNISINOS.

[5] MENEZES, Ricardo. Dicas de Segurança para sua rede Wireless. Disponível em: http://www.mobilezone.com.br/artigo6.htm 20/05/2007.

[6] Tutorial Rede Wireless. (2006) Disponível em: http://www.babooforum.com.br/idealbb/view.asp?topicID=269602. Apostila, 20/05/2007.

[7] MATOS, Luis. Guia Profissional de Redes Wireless. São Paulo, Editora Digerati Books, (2005).

[8] http://www.mytwt.net/ipca_arqcomp/myfiles/mydocuments/aulas/10Aula.pdf 25/05/2007.

[9] http://www.juliobattisti.com.br/tutoriais/paulocfarias/redesbasico003.asp 20/05/2007.

[10] ROSS, John - Wi-Fi, instale, configure e use redes Wireless (Sem – Fio), Editora ALTA BOOKS.

[11] ZANETTI, Alberto René; GONÇALVES, Leandro de Carvalho - *"Redes Locais sem Fio"*, On–line: http://www.dc.ufscar.br/~carvalho/WLAN/, Universidade Federal de São Carlos, Acessado em 20/05/2007.

[12] www.apostilando.com, acessado em 19/07/2007.

ANEXO I

A - CONFIGURANDO REDES SEM FIO PARA WINDOWS

Em um mundo ideal de redes, seria possível conectar um adaptador de rede ao computador, ligá-lo e se conectar à rede imediatamente. Normalmente, antes de poder transportar dados através de uma WLAN, tem que informar exatamente como e onde encontrar a rede e como conectar à Internet.

Este capítulo contém uma explicação sobre os conceitos gerais envolvidos com o funcionamento do Windows em uma WLAN e os procedimentos específicos para configurar as ferramentas e recursos de rede em diferentes versões do Windows.

No XP, tudo deve ocorrer automaticamente, desde que (e este é um fator preponderante), o adaptador de rede contenha um firmware compatível com a ferramenta de configuração automática do Windows.

Em configuração de redes Windows, não deve encontrar problemas com o *wireless*. Infelizmente, o Windows espalha as opções de configuração sobre todo o mapa virtual, portanto um conjunto de indicações para cada uma dessas opções pode ser extremamente útil.

A.1 CONFIGURAÇÃO GERAL DE REDE NO WINDOWS

Diferentes versões do Windows usam ferramentas de configuração diferentes mas todas com o mesmo objetivo: as configurações de endereço IP, máscara de sub-rede e endereço de gateway do computador devem combinar com os valores requeridos pelo resto da rede.[10]

A.1.1 - Dando um nome ao seu computador

Para os usuários, normalmente, é mais fácil guardar um nome do que um endereço IP para efeito de identificação. Portanto, deve atribuir um nome a cada computador na rede. Este nome aparecerá em todos os diretórios e listas de computadores que podem ser alcançados através da sua rede. Cada computador deve ter um nome único, com um comprimento máximo de 15 caracteres e espaços. O Windows também proporciona um espaço para a atribuição de cada computador da rede a um *workgroup*. [10]

Em algumas redes *wireless*, o nome do workgroup deve ser o mesmo que o SSID usado pelo ponto de acesso, especialmente quando o utilitário de configuração não exibe uma lista das redes próximas. Se estiver tendo problema com a conexão, tente alterar o nome do workgroup para o SSID da rede à qual deseja se associar.

A.2 CONFIGURANDO O WINDOWS 98 E O ME

O Windows 98, o 98SE e o ME, possuem ferramentas de configuração de rede similares.
Para definir o endereço IP e a máscara de sub-rede:

1. No Painel de Controle, clicar sobre o ícone Rede;
2. Na guia Configuração, selecionar o adaptador de rede e clicar sobre o botão Propriedades;
3. Clicar na guia Endereço IP;
4. Se o servidor de DHCP estiver ativo, selecionar a opção Obter um Endereço IP Automaticamente. Se não estz usando um servidor de DHCP, escolha a opção Especificar um Endereço IP e digitar o endereço IP atribuído a este computador no campo Endereço IP;
5. O campo Máscara de sub-Rede está localizado logo abaixo do endereço IP. Não usando um servidor de DHCP, digitar a mesma máscara de sub-rede que é usada pelo AP.

A.2.1 Gateway

Etapas para definir o endereço do gateway:

1. Na mesma janela usada para definir o endereço IP, clicar sobre a guia Gateway;
2. Digitar o endereço IP da LAN do ponto de acesso *wireless* no campo n*ovo* gateway e clicar no botão Adicionar; [10]

A.2.2 Servidores de DNS

Para definir as opções de DNS:

1. Na mesma janela usada para definir o endereço IP, clicar sobre a guia Configuração DNS;
2. Se um servidor de DHCP atribui endereços de DNS a clientes, selecionar a opção Desativar DNS; Se a rede usa um servidor DNS estático, selecionar a opção *Ativar* DNS;
3. Se ainda não estiver visível, digitar o nome atribuído a este computador no campo Host;
4. Se a LAN, o AP ou o servidor de DHCP, usa um nome de domínio, digitar o nome de domínio no campo Domínio;
5. Digitar o endereço de cada servidor de DNS usado pela sua rede no campo Ordem de Pesquisa Servidor DNS e clicar sobre o botão Adicionar. O gerente de sua rede ou o provedor de Internet pode fornecer os endereços de DNS corretos para a sua rede;
6. Clicar sobre o botão OK na janela Propriedades de TCP/IP e novamente na janela de Rede para salvar as novas configurações.

A.2.3 Opções do adaptador de interface de rede

Para alterar as configurações de interface de rede:

1. No Painel de Controle, clicar sobre o ícone Rede;

2. Na guia Configuração, selecionar o adaptador de rede e clicar sobre o botão Propriedades;
3. Clicar sobre a guia Avançado;
4. Selecionar cada um dos itens na lista de propriedades para ver a definição atual no campo Valor;
5. Após feitas as alterações necessárias clicar sobre o botão OK para salvar suas alterações e fechar a janela. Clicar no botão OK da janela Rede para voltar ao desktop. Alguns adaptadores de rede *wireless*, incluindo os produtos da Orinoco, não aceitam nenhuma opção de configuração.

Se não vir uma guia Avançado na janela Propriedades do Adaptador, usar o programa utilitário de configuração do fornecedor.

A.2.4 Identidade de rede

Antes de poder conectar a uma rede, deverá atribuir um nome ao computador. No Windows 98 e ME, as opções de configuração estão localizadas na guia Identificação da janela Rede. Seguir estes passos para alterar essas configurações:

1. No Painel de Controle, clicar sobre o ícone Rede;
2. Clicar sobre a guia Identificação;
3. Digitar o nome que identifica este computador na rede, no campo Nome do Computador;
4. Digitar o SSID da rede no campo Workgroup;
5. Se quiser oferecer uma descrição mais detalhada, preencha o campo Descrição do computador;
6. Feitas as alterações necessárias clicar sobre o botão OK para salvar suas alterações e fechar a janela. Clicar no botão OK da janela Rede para voltar ao desktop. [10]

A.3 CONFIGURANDO O WINDOWS 2000

O Windows 2000 possui as mesmas opções de configuração que as versões anteriores, mas algumas delas estão localizadas em diferentes locais.

A.3.1 Endereço IP e máscara de sub-rede

Siguir estes passos para definir o endereço IP e a máscara de sub-rede:

1. No Painel de Controle, clicar sobre o ícone Rede;
2. O perfil de conexão com a rede para a conexão Ethernet *wireless* a *Local Area Connection*. Clicar com o botão direito sobre o ícone e selecionar Propriedades no menu pop-up. Na janela que se abrirá, deve confirmar se o nome do adaptador de interface de rede estará visível no campo Usando Conexão;
3. Na lista de itens instalados, selecionar o item *Internet Protocol* (TCP/IP) e clicar sobre o botão Propriedades;
4. O servidor de DHCP estiver ativo, selecionar a opção Obter um Endereço IP Automaticamente. Não usando um servidor de DHCP, escolha a opção Usar o Endereço IP Seguinte e digitar o endereço IP atribuído a este computador no campo Endereço IP;
5. O campo Máscara de sub-Rede está localizado logo abaixo do endereço IP. Não usando um servidor de DHCP, digitar a mesma máscara de sub-rede que é usada pelo AP;
6. Digitar o endereço IP da LAN do ponto de acesso *wireless* no campo *GatewayDefault*;
7. Um servidor de DHCP atribui endereços de DNS a clientes, selecionar a opção Obter Endereço do Servidor DNS automaticamente. A rede usando um servidor DNS estático, selecionar a opção Usar os seguintes Endereços de Servidores DNS, e insira os endereços de DNS fornecidos pelo gerente da rede ou pelo provedor de Internet.

A.3.2 Compartilhamento de arquivos e impressoras

Funciona de forma idêntica ao compartilhamento de arquivos e impressoras das redes com fio.

Seguir os passos para alterar as opções do adaptador de rede:

1. No Painel de Controle, clicar sobre o ícone Rede e Conexões Dial-Up;
2. Clicar com o botão direito sobre o ícone do perfil da conexão *wireless*. Escolha Propriedades no menu pop-up;
3. Na guia Geral, clicar sobre o botão Configurar;
4. Clicar sobre a guia Avançado;
5. Selecionar cada um dos itens na lista de propriedades a definição atual no campo Valor;
6. Feitas as alterações necessárias clicar sobre o botão OK para salvar as alterações e fechar a janela. Clicar no botão OK da janela Rede para voltar ao desktop.

Alguns adaptadores de rede *wireless*, incluindo os produtos da Orinoco, não aceitam nenhuma opção de configuração.

Não havendo um guia Avançado na janela Propriedades do Adaptador, usar o programa utilitário de configuração do fornecedor. [10]

A.3.3 Identidade de rede

As configurações da opção de identificação no Windows 2000 estão localizadas na guia Identificação da Rede da janela Propriedades do Sistema. Seguir os passos para alterar essas configurações:

1. No Painel de Controle, clicar sobre o ícone Sistema;
2. Clicar sobre a guia Identificação da Rede;
3. Clicar sobre o botão Propriedades para abrir a janela Alteração de Identificação;
4. Digitar o nome que identifica este computador na rede, no campo Nome do computador;
5. Digitar o SSID da rede no campo Workgroup;
6. Clicar no botão OK para salvar suas alterações e fechar a janela.

A.4 CONFIGURANDO O WINDOWS XP

A Microsoft introduziu o suporte específico para redes 802.11b no Windows XP, que supostamente integra a configuração *wireless* com outras configurações do Windows. Teoricamente, isto pode facilitar a configuração e utilização de redes *wireless,* mas este ainda não é um processo *Plug-and-Play* simples.

O objetivo é a configuração *wireless* automática; o Windows deve detectar automaticamente o adaptador de rede e procurar por sinais de rede *wireless* acessíveis. Quando detecta uma rede próxima, o Windows deve permitir que um usuário se associe à rede apenas com alguns clicars de mousar. [10]

A.4.1 Status de conexão de rede *wireless*

Para abrir a janela de status, dê um clicar duplo sobre a rede ícone na barra de status. A janela Status de conexão da rede *wireless* mostra o estado atual do seu link, incluindo o status da conexão, a quantidade de tempo em que o link atual esteja ativo, a velocidade de transferência de dados, a qualidade do sinal e o número de bytes que foram enviados e recebidos pelo adaptador, desde que o adaptador se conectou a rede.

Para desabilitar o link de rádio, clicar sobre o botão Desabilitar na parte inferior da janela de status. Alterarando as configurações de rede mais comuns, clicar sobre o botão Propriedades. [10]

A.4.2 Definições da configuração da rede

Definindo as opções de configuração da WLAN, selecionar *Start * Settings * Network Connections* e dê um clicar duplo sobre o ícone da sua conexão *wireless*. Para configurar a sua conexão *wireless* seguir estes passos:

1. Na lista de itens instalados, selecionar o item *Internet Protocol* (TCP/IP) e clicar sobre o botão Propriedades. Clicar sobre a guia geral se ela ainda não estiver selecionada;
2. Se o servidor de DHCP estiver ativo, selecionar a opção Obter um Endereço IP Automaticamente. Se não estiver usando um servidor de DHCP, escolha a opção Usar o Endereço IP Seguinte e digitar o endereço IP atribuído a este computador no campo Endereço IP;
3. O campo Máscara de sub-Rede está localizado logo abaixo do endereço IP. Não usando um servidor de DHCP, digitar a mesma máscara de sub-rede que é usada pelo AP;
4. Digitar o endereço IP da LAN do ponto de acesso *wireless* no campo *GatewayDefault*;
5. Um servidor de DHCP atribui endereços de DNS a clientes, selecionar a opção Obter Endereço do Servidor DNS automaticamente. A rede usa um servidor DNS estático, selecionar a opção Usar os seguintes Endereços de Servidores DNS, e insira os endereços de DNS fornecidos pelo gerente da rede ou pelo provedor de Internet;
6. Clicar em OK para salvar as configurações e fechar esta janela. [10]

A.4.3 Compartilhamento de arquivos e impressoras

Funciona de forma idêntica ao compartilhamento de arquivos e impressoras das redes com fio.

Para alterar as opções do adaptador de rede:

1. Na janela Propriedades da conexão de rede sem fio, clicar sobre o botão Configurar;
2. Clicar sobre a guia Avançado;
3. Selecionar cada um dos itens na lista de propriedades para verificar a definição atual no campo Valor;
4. Feitas às alterações necessárias clicar sobre o botão OK para salvar alterações e fechar a janela. Clicar no botão OK da janela Rede para voltar ao desktop. Alguns adaptadores de rede *wireless*, incluindo os produtos da Orinoco, não aceitam nenhuma opção de configuração. Não havendo um guia Avançado na janela Propriedades do Adaptador, usar o programa utilitário de configuração do fornecedor.

A.4.4 Identidade de rede

Definir ou alterar o nome atribuído ao computador no Windows XP, abra a guia Nome do computador da janela Propriedades do Sistema. Seguir estes passos para alterar as definições:

1. No Painel de Controle, dê um clicar duplo sobre o ícone Sistema;
2. Clicar sobre a guia Nome do computador;
3. Digitar o nome que identifica o computador, no campo Descrição do computador;
4. Clicar no botão Alterar;
5. Digitar o SSID da rede no campo Workgroup;
6. Clicar sobre o botão OK para salvar as alterações e fechar a janela. [10]

A.5 CONFIGURANDO A REDE *WIRELESS* NO WINDOWS XP

As ferramentas de configuração do XP destinam-se a ser uma interface comum capaz de controlar muitas marcas de adaptadores de rede. Para a janela de Propriedades da conexão da rede sem fio:

1. Dê um clicar duplo sobre o ícone Rede na barra de status do Windows, próximo ao relógio no canto inferior direito da tela;
2. Clicar sobre o botão Propriedades na parte inferior da janela.

A.5.1 Selecionando uma rede

O computador estando dentro do intervalo de mais de uma rede, deve escolher a que deseja usar. O utilitário Propriedades Sem Fio inclui uma lista de redes preferidas, mas não o limita às redes que constam na lista.

A lista de redes disponíveis na janela Propriedades mostra os SSIDs de todas as redes que aceitarão um link a partir do adaptador *wireless*. Se o adaptador detectar apenas uma rede, o Windows automaticamente se conectará àquela rede. Quando um adaptador detecta mais de uma rede, ele comparará o SSID de cada rede aos nomes na lista de Redes Preferidas e o conectará automaticamente à rede com a prioridade mais alta. Pode alterar a ordem na qual o Windows procura as redes com os botões Mover para cima ou Mover para baixo na janela Propriedades.

A Microsoft ocultou cuidadosamente a caixa de diálogo que especifica se o Windows se limitará, ou não, às redes na lista de redes preferidas. Se o seu adaptador detectar uma rede que não esteja na sua lista de preferidas, ele configurará uma conexão, se a opção não-preferida na janela Avançada estiver ativa. Clicar sobre o botão Avançado na janela Propriedades para abrir essa janela.

Evidentemente, é possível que o computador venha a fazer a escolha errada. Quando isso acontecer, selecionar o SSID da rede correta na lista de Redes Disponíveis e clicar sobre o botão Configurar. Isso abrirá outra janela com mais informações sobre a rede, e configurará uma conexão para essa rede. [10]

A.5.2 Ativando ou desativando a criptografia

A janela Propriedades Locais, que pode ser aberta na janela de Propriedades principais com o botão Configurar ou o botão propriedades, inclui um conjunto de opções de criptografia WEP. Se estiver usando uma rede com a criptografia WEP ativa, ativar a opção *Data Encryption*. [10]